Advantage
Danske Bank

Staying ahead of the fraudsters

Patrick Keown
Fraud Operations Manager

28 February 2024

Agenda

- Fraud Landscape
- Who are the fraudsters?
- How the Bank protects businesses
- How fraudsters target businesses
- Most common scams
- Fraud strategy
- Signpost to external sources

Fraud Landscape

Business Cases:
Up 30%

Stolen: £580m → Cases: 1.38m → 3.2m stolen everyday → 7,400 victims per day

Conclusions:

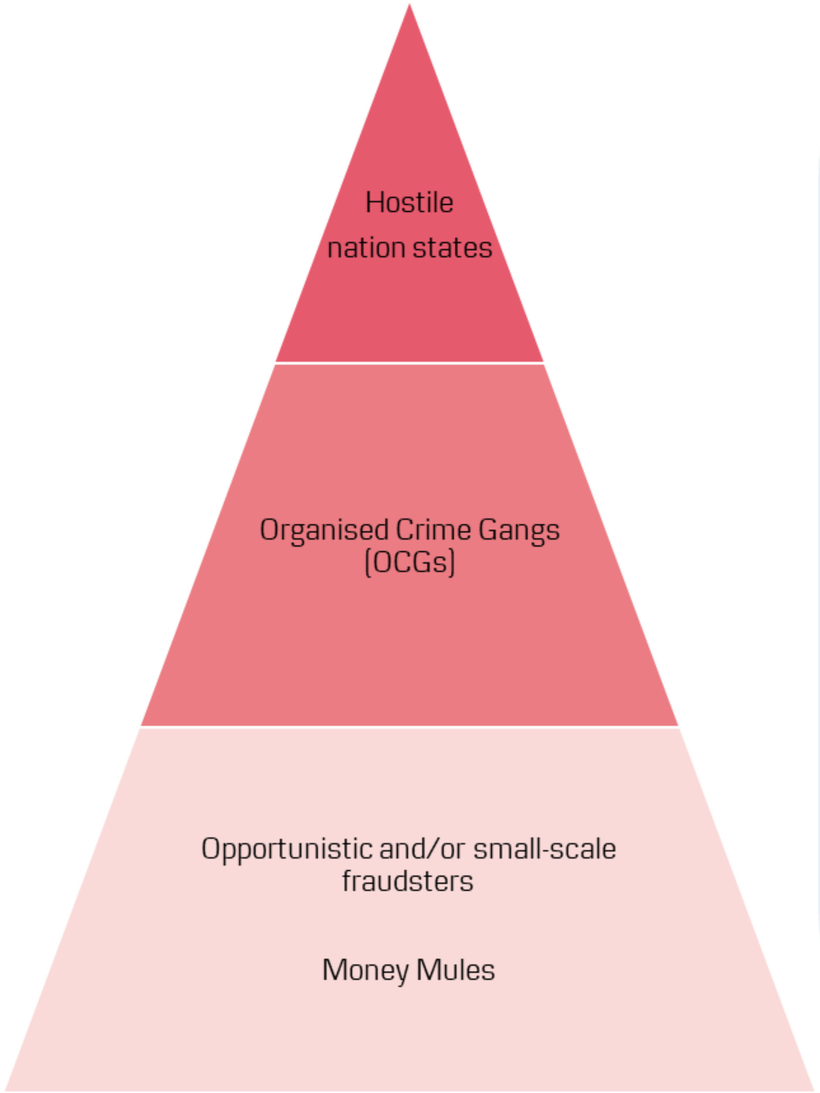
- The most likely crime you will fall victim to in the UK
- Sophisticated, well-funded and organised

Northern Ireland (Dec 2022 to Jan 2024):

- Stolen: £23m
- Cases: approx. 5,400

Source: UK Finance, 2023 Half Yearly Fraud Update, October 2023 & PSNI Fraud Data, 2023

What do we know about the fraudsters?



Graeme Bigger, Director General of the National Crime Agency, NCA's Annual Assessment, July 2023:

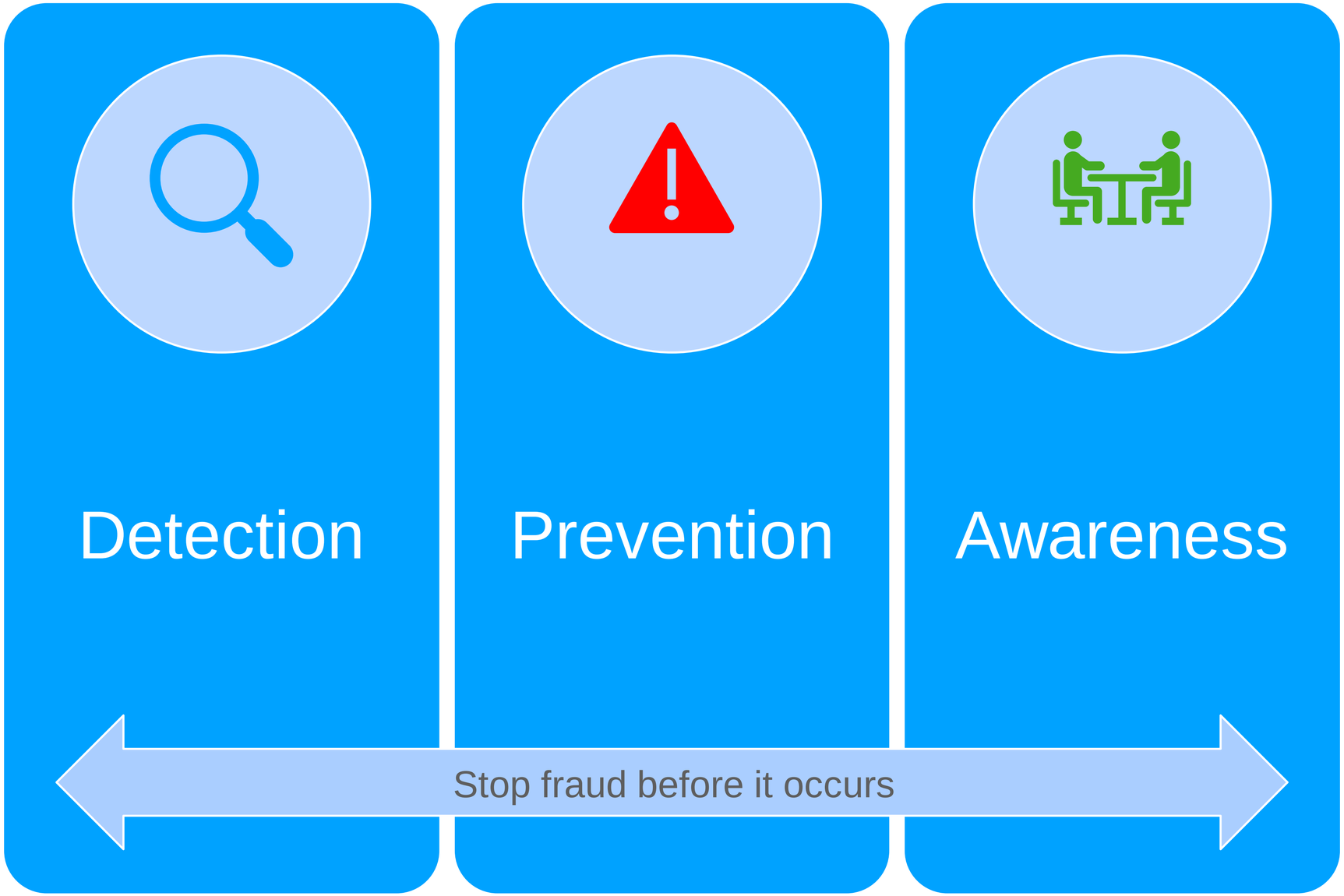
- "59,000 people involved in serious organized crime in the UK"
- "£12bn generated by criminal activities each year"
- "£100bn of dirty cash from around the globe laundered through the UK"

- "75% of fraud is partially or fully committed from overseas"
- "Emerging links to hostile states (e.g., North Korea and Russia) who use OCGs as proxies"

- Over 17,000 reports of money mule activity in H1 2023
- 23% involved young people aged 21 and under
- 64% involved people aged up to 30

Protecting customers

Advantage
Danske Bank



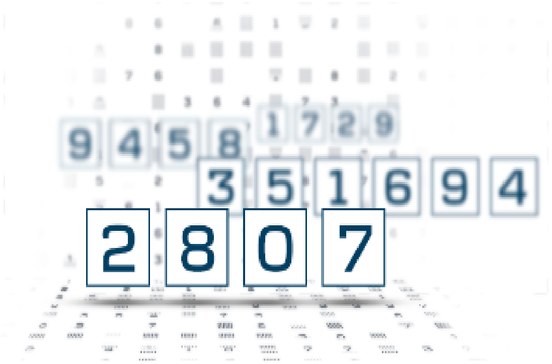
Protecting customers

Advantage
Danske Bank

Integrated security in District

Inbuilt security features ensure that:

- ✓ We can identify you before we disclose confidential information
- ✓ No unauthorised persons can access your company's data through District
- ✓ Your data is encrypted during transmission between your browser and Danske Bank



Two-step authentication with eSafeID

When you access District, we ask you for your password and a security code provided by your eSafeID device.

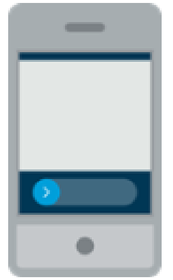
We use the most advanced security mechanisms to protect you, but to keep the high level of security and avoid fraud attempts you should use all available security features within District.

WEBROOT SecureAnywhere

Free Webroot Secure Anywhere®

Webroot Secure Anywhere® is available free to all District customers. It uses worldwide Webroot © Intelligence to identify new files, classify threats in real time, prevent browser attacks, remove viruses from your PC, and defend against financial and data-theft malware.

Download Webroot Secure Anywhere



Confirmation of Payee

Confirmation of Payee (CoP) means that we will ask you for the name of the person or business you are paying as well as account number, sort code and account type when you are making a payment through Mobile Bank. For more information on the responses you may see and our advice for each response go to our Confirmation of Payee page.

Strength through partnerships

Advantage
Danske Bank

UK FINANCE

cifas
Leaders in fraud prevention

PSR

pay.uk

Ofcom

VOCALINK
mastercard

scamwiseNI
PARTNERSHIP

TAKE FIVE TO STOP FRAUD

MEF
MOBILE ECOSYSTEM FORUM

experian

POLICE SERVICE NORTHERN IRELAND

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

DCPCU
Dedicated Card and Payment Crime Unit

National Cyber Security Centre
a part of GCHQ

CITY OF LONDON POLICE

We partner with key stakeholders at a local and national level:

- Regulatory
- Specialist experts
- Intelligence gathering and sharing
- Communication and awareness
- Law Enforcement

Fraud typology

Fraud comes in many forms, but at a high level there are two types:

Unauthorised: occurs without the victims knowledge

Authorised: victim is manipulated into being an ‘enabler’ to fraud

Avg. Gross Unauthorised Fraud Loss in H1 2023	£270
Avg. Gross Authorised Fraud Loss in H1 2023	£2,057

UK FINANCE

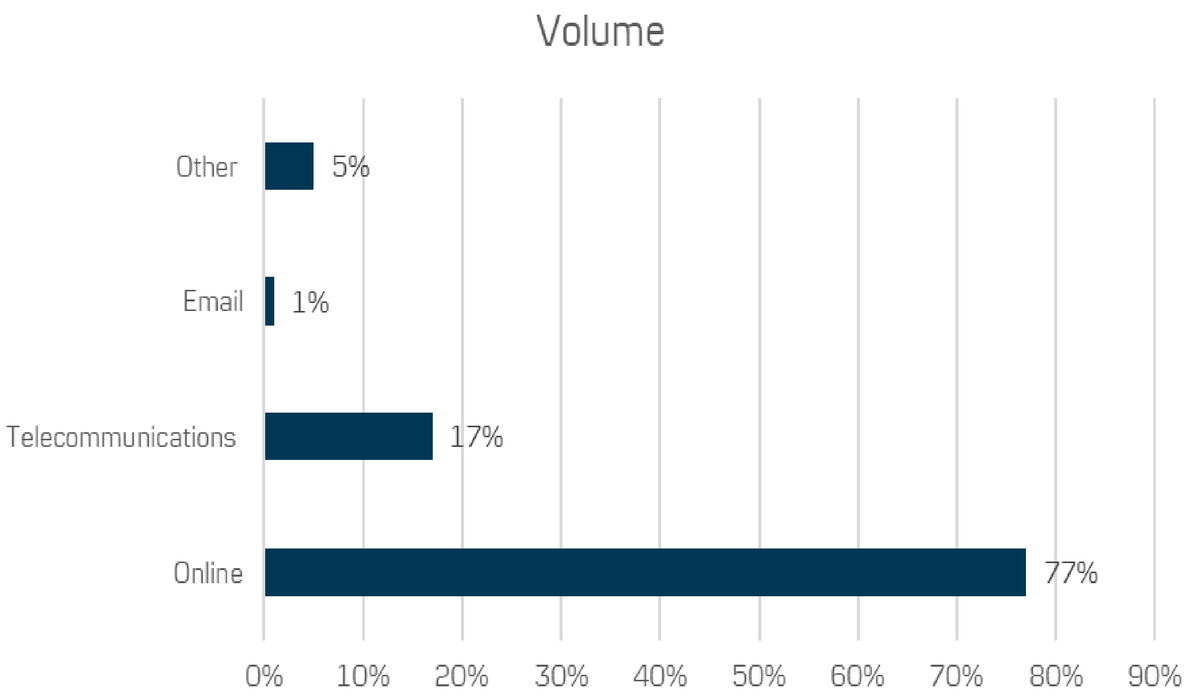
Where fraud starts...

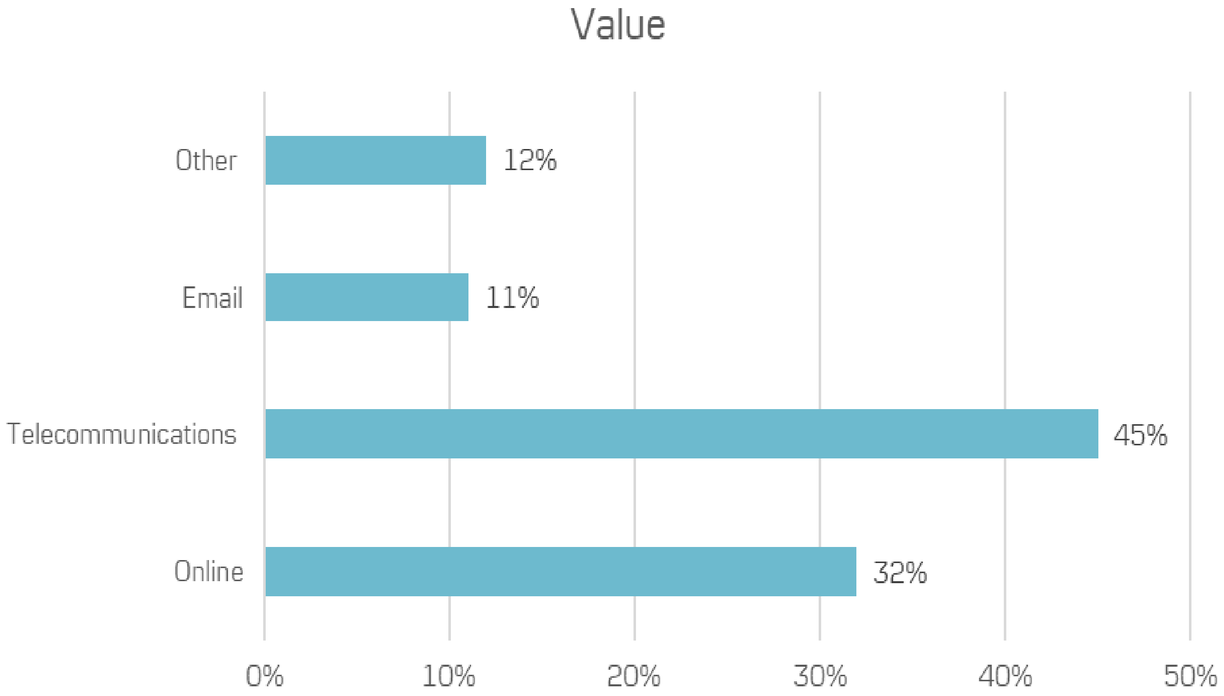
Common ways fraudsters get business data:

- Data Breach
- Research your business – website, LinkedIN, Social channels, Companies House
- Phishing and Smishing – we give it to them

Where fraud starts...

Source: UK Finance, 2023 Half Yearly Fraud Update, October 2023





- Vast majority of scams start online – e.g., fake adverts on online platforms such as Facebook, Instagram, Tik Tok, Google
- Fraud originating from telecommunications (telephone, text messages, Whatsapp) is where victims lose the most money – active social engineering
- **Fraud originating via email has a disproportionately large financial impact compared with how often it happens – mostly linked to businesses**

How fraudsters target businesses...

Advantage
Danske Bank

Phishing	Criminals sending an email pretending to be a trusted source
Vishing	Criminals calling pretending to be a trusted source
Number Spoofing	Technique used by fraudsters to manipulate the caller ID displayed on your phone, making it appear the call is coming from a trusted source
Remote Access Software	Allows fraudsters to view, access, and control a computer or device from a remote location. Typically requires installation on the device via a software download. When active this software means the fraudster has full access to the computer or device.

How fraudsters target businesses...

Advantage
Danske Bank

- Phishing
- Vishing
- Number Spoofing
- Remote Access Software

Danske Bank

NCA National Crime Agency

HM Revenue & Customs

Microsoft

Google Workspace

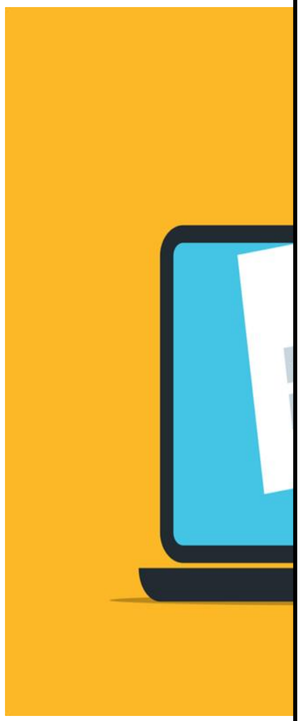
Outlook

Gmail

third party suppliers, clients, partners, employees

Phishing – the most common attack method on business

Advantage
Danske Bank



Hi Patrick,

Your password is about to expire in 48 hours. Please renew it by clicking on the link below:

Change Password Link

Regards,
Microsoft Team

Microsoft Corporation | One Microsoft Way Remond, WA
98052-6399

This message was sent from an unmonitored email address.
Please do not reply to this message.

Privacy | Legal

Microsoft

s them
nt.
icrosoft,

ok,

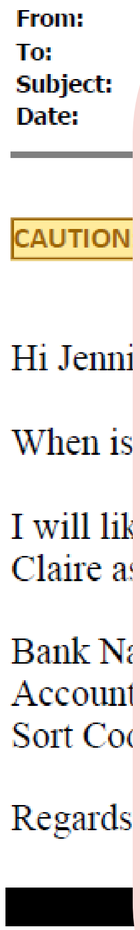
Invoice re-direction / Mandate fraud

Third P

Invoice redirection fraud

- Criminals will gain access to an employee's mailbox – either in your business or that of the third party.
- They set up “mail rules” to divert emails to hidden folders to review communications, before releasing the emails into your inbox.
- They do their homework and have a plan- they will read all emails and work out when to expect payments
- They will wait for as long as it takes for on invoice or payment request – then they will alter the beneficiary details meaning the money is sent to an account they control
- Alternatively, they will impersonate a known supplier or payee, and ask you to amend the beneficiary details on your records meaning the next time you pay them the money goes to an account they control.
- They may send “phishing” emails from your inbox to all your contacts

Payroll Re-direction…….


From:
To:
Subject:
Date:

CAUTION

Hi Jenni

When is

I will lik
Claire a

Bank Na
Account
Sort Coc

Regards

[redacted]

Sent from

£24.8 million

Lost during H1 2023 to Invoice Re-Direction Scams

Preventing Invoice redirection scams

- Be wary of emails or text messages claiming to be from a supplier or known third party advising of a change of account details
- Verbally confirm the authenticity of any requests to amend beneficiary account details of a payee or supplier
- Verbally confirm the accuracy of the beneficiary details with the intended recipients before sending payments
- Dual authorisation on payments

Case Study: Bank impersonation

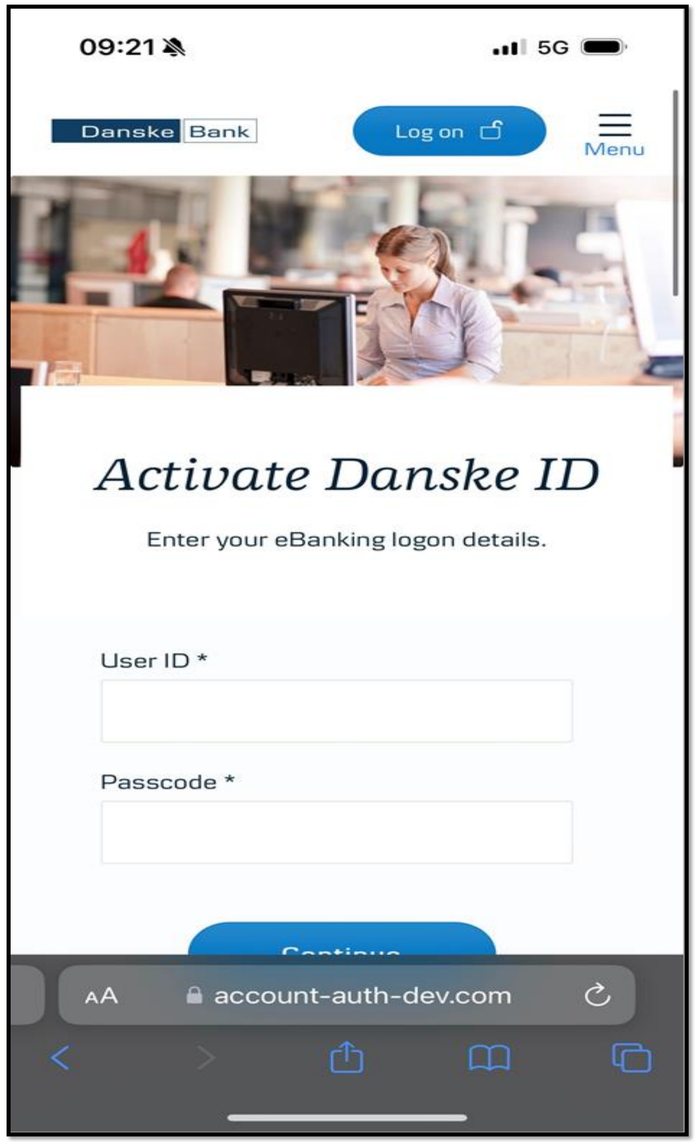
Advantage
Danske Bank

Bank impersonation scams are becoming more prevalent

The tactics used by fraudsters are becoming more sophisticated

Multiple Banks reported similar cases towards end of January 2023:

1. Vishing – “Your banks fraud/security team calling…”
2. Social Engineering (1) – “suspicious activity on online banking, urgent!!”
3. Fake Website which included ‘Click to Chat’
4. Remote Access Software – “let us help you secure your accounts”
5. Fraudulent payments created
6. Social engineering (2) – “we need a second colleague to help us”
7. Repeat steps 2 - 5
8. Fraudulent payments completed



Examples of fake web address:

helpdanskedistrict.web.app

danskebankhelp.web.app

supportwithdanske.web.app

danskebusinesschat.web

account-id-auth.com

account-id-authenticate.com

account-setup-id.com

review-alert-account.com

now-sec-mobile.com

account-auth-dev.com

Official website:

www.danskebank.co.uk

Ransomware

Ransomware attacks against UK businesses are increasing

Protect computers and devices

- Install antivirus software and a firewall
- Run full virus scans (monthly)
- Antivirus updates (weekly)
- Install recommended OS and program updates
- Be wary of unexpected emails/text messages containing attachments
- Use strong and unique passwords and update regularly
- Protect user access by enabling 2FA

Consequences of fraud...

The impacts of fraud can be far reaching…

- Financial
- Reputational: customer and third-party relationships, data related: ICO and/or press scrutiny
- Emotional: Impact on leaders and on staff
- Future – How will this impact your plans?

What to do if you are a victim of fraud...

Report to…

1. Your Bank

- Telephone: 0800 917 7657 (24/7) or Relationship Manager
- Website: https://danskebank.co.uk/personal/help/reporting-fraud-and-unauthorised-transactions
- Email: ukfraudteam@danskebank.co.uk

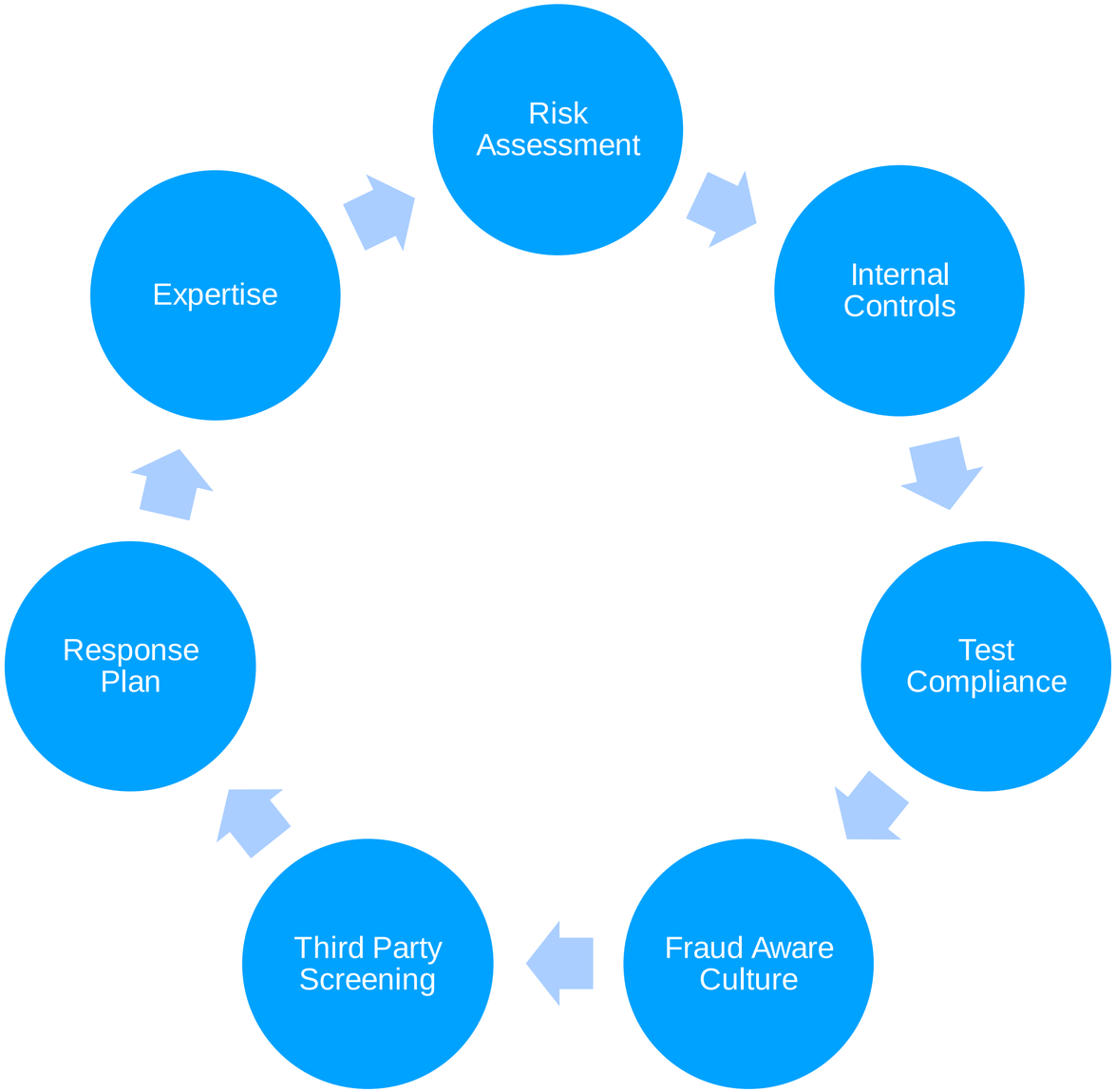
2. PSNI on 101

3. Action Fraud via https://www.actionfraud.police.uk/

Fraud Strategy

You need to define your strategy to suit your business, but some things to consider:

- Identify potential fraud risks – think data and payments
- Implement internal controls
- Regularly test compliance of controls and apply learnings
- Embed a fraud aware culture including employee training
- Consider the fraud and cyber awareness of your third-parties/supply chain
- Develop a response plan
- Get expert help if needed e.g., IT Support



Best practice advice to keep your business safe

Advantage
Danske Bank

Be sceptical

Verbally confirm payee account details – first time payment or following a change request

Use Confirmation of Payee to check beneficiary details are correct

Employ dual authorisation of payments on District

Keep antivirus software up to date

Do not use business email address for personal reasons

Report suspicious emails

Unsure of who you are talking too? Just hang up

Sources of advice and guidance

Advantage
Danske Bank

National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

TAKE FIVE TO STOP FRAUD™

https://www.ncsc.gov.uk/section/advice-guidance/all-topics

https://www.ncsc.gov.uk/cyberessentials/overview

https://www.takefive-stopfraud.org.uk/

Thank you.