Deutsche Bank
Corporate Bank

Fraud Prevention & Cyber Security

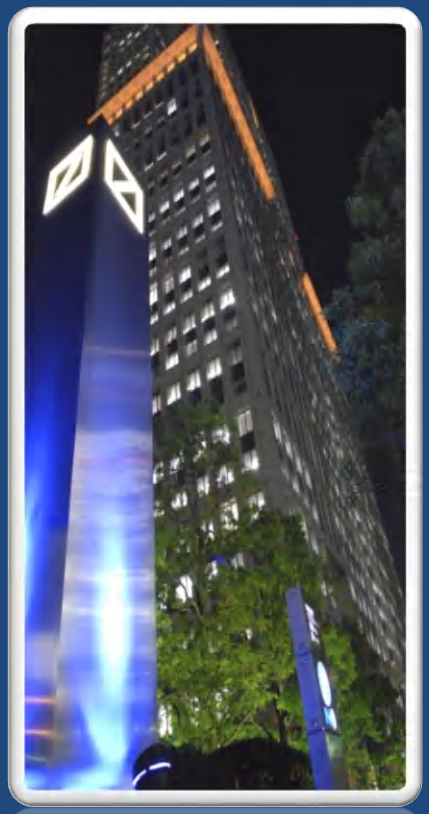
Delivering fraud protection and cyber security for our clients

- #PositiveImpact

150 YEARS

March
2020

Contents:



Introduction:

Fraud and cyber enabled crime is increasing and remains a significant threat to all businesses regardless of the size, location or the industry they operate in. Significant amounts of money are lost to fraud, therefore it is important that businesses understand and manage the fraud risks they are exposed to.

This brochure is designed for businesses to help protect themselves against fraud.

It details some of the common risks they may face, along with ideas about how to manage them. It should be shared with employees from across the organisation, so that they are aware of the threats and the role they play in preventing fraud.

Please contact your Relationship Manager if you have any questions or require further information about the content of this brochure.

Fraud Awareness:

The risks faced by each organisation are different and are constantly evolving, this brochure should complement, not replace a business's regular fraud risk assessment.

Criminal actors today, tomorrow and going forward will continue to find innovative new ways to target organisations and individuals. With the age of digitalisation crime is moving away from the traditional typologies. The UK National Crime Agency[1] state on their website: "Cyber crime continues to rise in scale and complexity, affecting essential services, businesses and private individuals alike. Cyber crime costs the UK billions of pounds, causes untold damage, and threatens national security".

Organisations across all industries are faced with the growing threat of fraud. Fraud losses are measurable, however the financial harm and potential reputational damage is more difficult to quantify.

It is important that all employees of an organisation receive fraud awareness training giving them a greater opportunity to recognise the threat and helping to build organisational integrity. Frequent training and the business keeping up to date with the latest fraud/cyber trends is important to increase the protection level. The threat can come from inside the business and those external to the organisation.

Employees must have a clear understanding of how and to whom they escalate any concerns.

How does your organisation deliver fraud awareness training and how often?

- During induction training.
- Frequently
- On-line
- Classroom
- Webinars
- External providers

[1]https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Financial Crime:

Financial Crime is an increasing concern for all financial institutions, from the largest global organisations to the smallest companies and partnerships. Preventing and detecting Financial Crime is rapidly evolving to be one of their biggest challenges, the impact of which extends well beyond monetary losses to reputation and brand, employee morale, business relations, as well as regulatory censure.

Organised Crime Groups:

Criminals do not operate in a vacuum. In the case of organised crime groups they are well organised, highly disciplined, cyber literate, determined and highly motivated. They will actively seek to employ any tactics to gain an advantage with the financial rewards sometimes running into the millions.

Financial inducements are one way of recruiting insiders, however threats to the person or to family members can be made. On occasions a member of a gang will secure employment within a business, so they become the insider, feeding an endless supply of confidential information to the crime group and gaining greater knowledge of the business and the sector they operate in.

Criminals have many other options available to commit fraud:

— Employees putting inappropriate personal information on social media including ill considered details of their jobs.

— Social engineering: criminals manipulating or tricking employees into revealing sensitive information. Current cyber threats against companies specifically involve phishing and spear-phishing attacks.

— Companies using social media without thinking of the consequences.

— Interception of the post, at a business and/or a customer address.

— Cyber attacks on the company and/or suppliers.

— On-line research into the company.

Internal Fraud:

While most staff have no intention of committing fraud it is important for businesses to understand their internal fraud risks and have appropriate controls in place to prevent it.

- Instill a fraud prevention culture by setting the tone from the top.
- Have a response plan to managing internal fraud incidents and educate employees about the consequences of committing fraud against the business.
- Undertake a regular fraud risk assessment, implementing controls to mitigate identified risks and test that the controls are working.
- Implement a robust onboarding process for new employees, along with undertaking proportionate ongoing and event driven checks throughout their period of employment.
- Set up a confidential reporting system for employees to report suspected fraud and misconduct anonymously and in confidence.
- Ensure a segregation of duties for processes that are assessed as having an increased risk of fraud, which should include processing payments.
- Ensure that only employees with a valid business reason have access to business banking records, internet banking passwords, cheque books and company credit cards.
- Have a strong and independent audit function.

According to PwC's Global Economic Crime and Fraud Survey 2018[2]
52% of all frauds are perpetrated by people inside the organisation.
(an increase from 46% in 2016)

The internal fraud risk faced by companies will not be the same and will depend upon a number of factors which include the industry that the business is operating in, their client base, the countries where they operate and the channels by which they conduct business. Some common fraud types which most companies will be exposed to are fraudulent expense claims and the misappropriation of company assets.

2. https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

Cheque Fraud:

A focus by banks on identifying lost or fraudulent cheques as they pass through the clearing system means that £9.50 in every £10 of attempted cheque fraud is stopped before a loss occurs.

However, a minority of fraudulent cheques do get through the system, and it is helpful if business know what kind of fraud is attempted so they can try to avoid falling victim.

- **Counterfeit:** A cheque that has been created on non-bank paper to look genuine. It relates to a genuine account, but has actually been created and written by a fraudster for the purposes of committing fraud.
- **Forgery:** A genuine cheque, however the signature is not that of the account holder. The fraudster has forged the signature by signing the cheque themselves.
- **Fraudulently altered:** A genuine cheque made out by the customer but it has been altered by a fraudster before it has been paid in (e.g. by altering the recipient's name on the cheque or the amount. It is no longer a genuine cheque).

How to protect your Business:

- Keep your cheque books in a secure place, with access limited to individuals who are required, as part of their role to issue cheques.
- Regularly review the list of individuals who are authorised to sign cheques, ensuring that the bank is immediately informed of any changes.
- Write the payee's name in full, for example 'John Smith' rather than 'J Smith' and cross through any space left in the amount or payee fields.
- Independently verify cheques issued against funds debited from the account. Notify the bank immediately of any discrepancies
- If you print your own cheques, use a reputable cheque printing firm.
- Never release goods until funds have cleared.
- Be sceptical of customers who overpay for goods and subsequently request the difference to be returned.

Social Engineering:

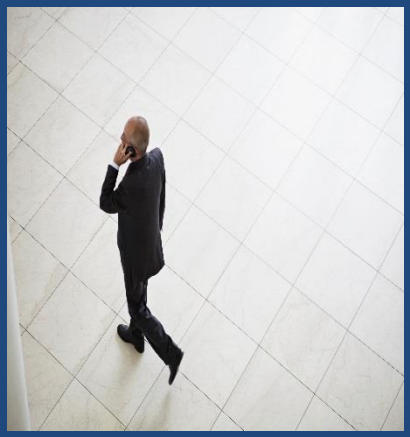
What is Social Engineering?

Is the act of manipulating an individual to provide information that they would not normally disclose. It relies upon human interaction and is often used by fraudsters to obtain confidential or sensitive information, for example online banking credentials.

It may also be used as a method to obtain seemingly innocuous information about a business or their employees, which may be used in the future to convince another individual to provide confidential information.

Why use Social Engineering?

It is often easier to obtain confidential information through social engineering than breaking in to a company's IT systems.



Social engineers obtain information by preying on four basic human emotions; fear, obedience, greed and helpfulness.

Social engineering approaches will often require urgent action, with either the promise of a reward or threat of a consequence. The fraudster may impersonate a law enforcement officer or a company executive, playing on the human Instinct to trust a person in authority. They may also be charismatic and exploit a person's willingness to help.

Social Engineering and social media:

Social media and business networking sites are often used by fraudsters to identify and research social engineering targets. These sites are used to build up knowledge of the business and its personnel, which will be used as part of the attack.

Businesses should consider implementing a social media policy to reduce the risk of information that is posted online being used as part of a social engineering attack.

Businesses should also be vigilant about the information it publishes about itself on the internet.

Spoofing:

Spoofed telephone numbers and email addresses can be used as part of a social engineering attack, to convince the victim that the enquiry is originating from a legitimate source.

Examples of spoofing include a different telephone number being displayed on the recipient's caller ID than the one that the call is originating from, or the sender's address displayed in an email being different from the address that actually sent it.

Similar email addresses could also be used to trick the recipient in to thinking that it is a genuine message for example replacing a lower case 'l' with a capital 'i' in the email domain.

Social Engineering Methodologies:

Social engineers will target victims through various channels, with it more common that the interaction will be remote rather than face to face. It is important that employees remain vigilant at all times about who they are disclosing information to. Common social engineering attacks include:

Email Phishing:

This is where individuals/employees receive emails directing them to websites where they are asked to provide confidential personal/company or financial information. Whilst these emails may appear to come from a legitimate site, these emails are designed to steal information and use it to access your accounts. Phishing emails can also include file attachments, which when opened could result in malware being installed on the recipient's device.

Vishing:

This involves a fraudster making phone calls to a company or individual posing as bank staff, the Police, regular supplier/client, internal technical support or other officials in a position of trust.

The call may be made to coerce a company financial controller into:

Sending their money to another account often purportedly for 'safe keeping' or 'holding'.

— Withdrawing cash and handing it over to the fraudster for investigation.

— Giving personal financial information, which can then be used to gain access to your bank accounts?.

To add a sense of legitimacy to the call the fraudster may spoof a genuine organisation's telephone number and then ask the victim to check the number displayed on the caller ID matches the one displayed on the company's website.

Spear Phishing Emails:

Phishers know that their success rate is much higher when they tailor their bait to the person they are targeting. So one of their methods is to pretend to be someone with whom you are currently in contact. This may be a colleague, a client or a business associate. Your colleagues email is john.james @gmail.com, however you fail to realise the email is from james.john@gmaill.com. (An extra "l" added).

This type of email has a personal feel, refers to an ongoing issue and may even use phrases that are familiar. As a result, you're unlikely to be as careful: you don't check the address used to send the email and you might open a malicious attachment or click on a link.

Smishing:

The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

Similarly, there are other social engineering techniques, like Tailgating, where a person takes help of an authorized person to get access to restricted areas where RFID authentication or some other electronic barrier is present.

Social Engineering — Examples:

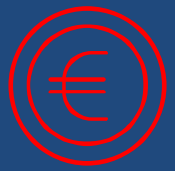
Example 1:

Late one Friday afternoon the CFO of ABC Ltd received a call from someone who identified themselves as an employee from the Payment Operations team of ABC Ltd.'s bank. The CFO was informed that there was an unusual debit on the company's bank account, which needed to be cancelled immediately by generating a code from the CFO's internet banking token.

The CFO was in a hurry to leave for the weekend, he generated the code and provided it to the caller.

The following Monday the CFO discovered an unauthorised payment of EUR 300K had debited the company's bank account on Friday.

ABC Ltd were informed by their bank that there was no record of a call being made to the CFO the previous Friday, and that the code he had generated had been used to authorise the payment from the account through online banking.



Example 2:

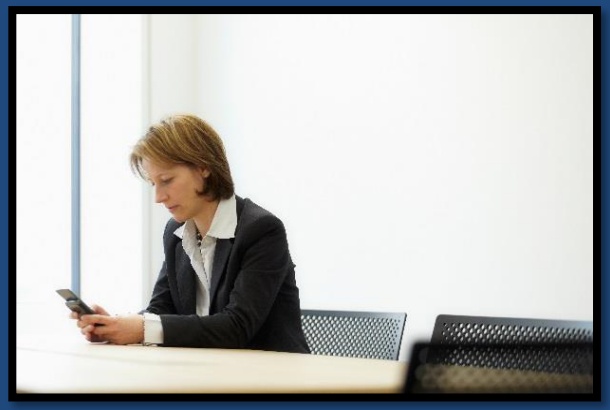
An accounts payable director at XYZ Ltd received an email claiming to be from their bank, advising that a software update was required to continue using their online banking.

The email contained a link to fake login screen. The director clicked the link and entered his online banking credentials in order to install the required software updates.

The fraudster was able to use this information to gain access to XYZ Ltd.'s online banking and change the beneficiary account numbers on existing payments, which were awaiting authorisation. The payments were subsequently authorised, as only the beneficiary names and not the beneficiary account numbers were checked by XYZ Ltd, resulting in a loss of EUR 500K to the company.

Social Engineering: General Guidance:

- Do not click on links or open attachments to emails from an untrusted or suspicious sender. If in doubt refer the email to your IT Security team.
- Examine emails for poor grammar and spelling, remember, if the email contains information about the company it does not mean it is genuine. If in doubt, always verify the request by contacting the individual using details obtained from an independent and trusted source.
- Never enter personal or confidential information to a site that has been accessed by a link from an unsolicited email.
- Independently visit web pages through your web browser instead of clicking on a link in an email, which may install malware on your device.
- If you receive an email with an unusual request, carefully examine the sender's email address has not been altered, for example abcltd.com has not been changed to abc1td.com. The email header can be reviewed to determine if the email address has been spoofed.
- If you receive an unsolicited SMS text message, do not click on links, or provide information, unless you are sure it is genuine.
- Always check who is requesting information from you, take your time to consider any request and never feel pressurised in to complying with it. If in doubt, contact the individual using details obtained from an independent and trusted source.



Tips for Management:

- Implement and enforce a social media policy.
- Have an internal process to report phishing emails and delete suspicious emails once reported.
- Be careful about the amount of information you post on social media and business networking sites. Do not publish any confidential information about your business and consider whether the names of your suppliers needs to be made available to the public.

Social Engineering: Payments Specific:

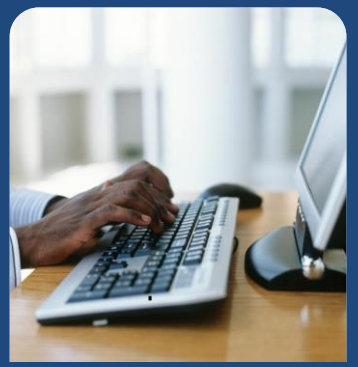
- When responding to an email requesting the transfer of funds, start a new email thread rather than replying to the email received.
- Have robust procedures for making payments, which should include verifying the legitimacy of any internal instructions and a four eyes principle.
- Orders should only be accepted and actioned via secure communication channels.
- Regularly reconcile bank accounts and immediately report to your Relationship Manager any transactions you do not recognise or suspect may be fraudulent.
- Establish single points of contact at suppliers for invoice queries.
- Use multi factor authentication to protect your accounts, payments and systems

- Always check requests to change bank account details with the supplier, using contact information obtained from an independent and trusted source
- Consider sending a confirmation to suppliers when payments are made, to enable any issues to be identified quickly.
- Implement and enforce a clear desk policy, which will include the secure storage and disposal of confidential information.
- Provide frequent training to employees about the risks of social engineering and common scams.

Business Email Compromise (BEC):

BEC or CEO fraud is a social engineering attack which remains a threat to businesses of all sizes globally.
It involves an email being sent to an employee, who is often someone working in accounts payable, requesting that an urgent payment is made. The email is often from an individual impersonating a senior employee within the business for example the CEO or CFO. To make the request appear more authentic the email will often include information about the business or use similar language to that used by the person they are impersonating. This information may have been sourced through social engineering, social media/business networking profiles, online research or by email hacking. The sender will either have spoofed the genuine employee's email address or used one very similar by changing a couple of characters. The request will often be time critical and the language will be persuasive, with a combination of the following elements:

- Use of authority: It is an order to do this.
- Confidentiality: This project is highly confidential, do not tell anyone else about it.
- Appreciation : I appreciate your support and it will be recognised in your year end appraisal.
- Pressure: The success of this project relies on this payment being made.



A variation of this scheme is that the email states that the employee will be contacted by a legal representative of the company working on a specific project and requesting them to follow their instructions.

Example:

It is a Friday afternoon and the senior accounts payable clerk receives an email purportedly from the CEO of their company.

The email address matches that of the CEO and the signature block looks the same. The email states that the CEO is travelling to China to close a deal, will be uncontactable and that an immediate international payment of USD 4M is to be made to an account held at a bank in China to ensure the contract is finalised. The email includes information about the importance of the project to the company and the implications for the company if the payment is not made that afternoon. The CEO states that the project is confidential and should not be discussed with anyone else in the company.

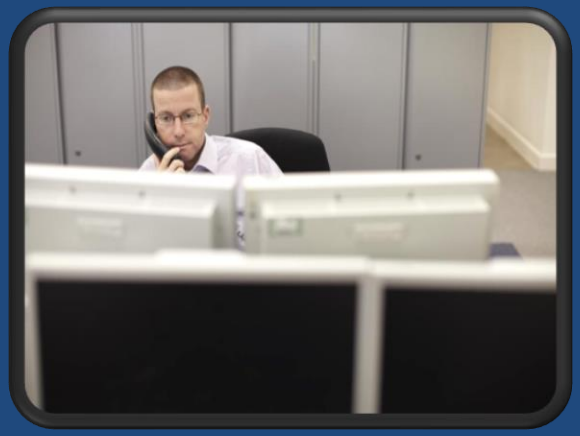
The employee acts upon the email and makes the payment.

On Monday morning, the payment is flagged as a potential concern.

Further investigation identifies that the CEO's email address had been spoofed by an external party and the payment request was fraudulent. No funds were recovered, resulting in a loss of USD 4M to the company.

Payment Diversion Fraud:

(Also known as Invoice Redirect and Mandate fraud)



Payment Diversion fraud is a type of social engineering attack where a criminal tricks a business into changing the bank account payee details for a payment. The criminal pretends to be a known regular supplier and informs the business of a change of bank account details. Standing order and direct debits can also be affected.

As with BEC/CEO Fraud, criminals will usually target the Finance or Accounts dept.
All business sectors have been hit, notably health, construction, manufacturing and transport.

The criminals will have researched their targets before the attack. For example via social media and open source research. They may have compromised email accounts or intercepted the postal mail and may have an insider in the business, so will know when invoices are sent, the format, and even previous invoice numbers. If this fraud is successful it may not be identified until much later when the genuine supplier chases for non-receipt of the payment, making it highly unlikely that any funds will be recovered.

A report published by UK Finance[3] on 25 March 2019, stated that in a survey of 1,500 UK businesses, UK Finance identified that more than four in ten of them were unaware of the risks posed by invoice fraud. Katie Worobec, Managing Director of Economic Crime at UK Finance said:

"Invoice fraud could happen to businesses of all sizes. It's vital that all employees are trained to identify potentially fraudulent transactions. The gangs behind this type of fraud are increasingly sophisticated and will often get hold of details that allow them to pose convincingly as regular suppliers."

Example:

ABC Inc is a construction company responsible for a new retail development, they have a billboard on site listing their suppliers and sub –contractors, one of which is XYZ Inc.

ABC Inc received a letter from XYZ Inc on letter headed paper advising of a change of bank account details.
ABC Inc updated their payments system, with the next payment for USD 350K sent to their new ABC Inc.'s new bank account.
10 days later XYZ Inc advised ABC Inc that the payment was still outstanding. Due to the time that had elapsed since the payment was made, no funds were recovered.

[3] https://ukfinancedrupal.westeurope.cloudapp.azure.com/news-and-insight/news-in-brief/news-brief-25-march-2019

Password Hacking:

Password hacking refers to the unauthorised procurement of passwords for devices, applications and services:

Impact:

Password hacking can result in any of the following unauthorized access: -

- Online bank and payments accounts.
- Business applications and systems.
- Business and personal email accounts, which can facilitate password resets for other online accounts.
- Online shopping accounts.
- Social media and business networking accounts.

Prevention:

- Use different passwords for all online accounts.
- Enforce strong passwords.
- Do not disclose passwords to other people or write them down.
- Change a password immediately, if it is suspected of being compromised.
- Don't save passwords on a network for example on Intranet pages or in Share Points.
- If necessary, use a 'password safe' to store personal passwords.
- Where available use 2FA when logging in to online accounts and verifying the identity of clients.

What is two factor authentication? (2FA)

2FA is an additional layer of security used to verify an individual's identity. This is done through two of the following independent components:

- Something they know, for example a password.
- Something they have, for example a token which generates a dynamic code.
- Something they are, for example a fingerprint.

Ransomware:

Ransomware is malware used to block access to files or encrypt data on a computer system. The purpose of ransomware is to extort money out of the victim in return for unlocking the files or decrypting the data. It is common for the fraudster to request the ransom payment in a crypto currency for example Bitcoin. However in recent cases, data is stolen before the encryption mechanism is installed so that the stolen data is used to put more pressure on the victim companies to pay, rather than restore from backups.

Types of Ransomware

Crypto Trojans:

Crypto Trojans encrypt files making them unreadable for the user. In exchange for a ransom, the user is offered the prospect that the files will be decrypted. A well-known example of a crypto Trojan is Locky.

Lock Screen Trojans:

Lock screen trojans do not affect the files themselves. Instead, they restrict the user's input options, preventing any further use of the computer. Usually a lock screen prevents the system from functioning properly.

How to protect your Business:

- Back up important data regularly on independent file systems
- Install all updates to software and systems.
- Implement a robust cyber-security framework.
- Carefully examine any email received, before opening an attachment or clicking on links . This should include assessing the credibility of the email, checking the language and grammar, considering whether any request in the email seems reasonable or normal. In addition check the sender's email address and consider the possibility it could have been spoofed or that characters in the address have been changed for example '1' instead of 'I'
- Be especially cautious about opening file attachments with the file extensions .asf, .exe, .avi, .mov, .mpg, .bat, .scr, .zip, .rtf, .doc, .pif, .reg and .vbs. Consider to automatically block some file extensions within your company.

Further Information on Fraud & Cyber Security

Latest cyber security and fraud advisory news can be found at:

- Take Five to Stop Fraud

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

- The Financial Fraud Action

  www.financialfraudaction.org.uk

- FBI – Common Fraud Schemes

  https://www.fbi.gov/scams-and-safety/common-fraud-schemes

- Action Fraud

  https://www.actionfraud.police.uk/

- Allianz für Cyber-Sicherheit German Language Only

  www.allianz-fuer-cybersicherheit.de

- US CERT

  https://www.us-cert.gov

- Association of Certified Fraud Examiner

  http://www.acfe.com/fraud-resources.aspx

- The Internet Crime Complaint Center

  www.ic3.gov

Disclaimer

This presentation is for information purposes only and is designed to serve as a general overview regarding the services of Deutsche Bank AG, any of its branches and affiliates. The general description in this (presentation, factsheet, brochure, newsletter) relates to services offered by the Global Transaction Banking of Deutsche Bank AG, any of its branches and affiliates to customers as of *October 2019* which may be subject to change in the future. This presentation and the general description of the services are in their nature only illustrative, do neither explicitly nor implicitly make an offer and therefore do not contain or cannot result in any contractual or non-contractual obligation or liability of Deutsche Bank AG, any of its branches or affiliates.

Deutsche Bank AG is authorized under German Banking Law (competent authorities: European Central Bank and German Federal Financial Supervisory Authority (BaFin) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and the BaFin, and to limited supervision in the United Kingdom by the Prudential Regulation Authority and the Financial Conduct Authority. Details about the extent of our authorization and supervision by these authorities are available on request.

This communication has been approved and/or communicated by Deutsche Bank Group. Products or services referenced in this communication are provided by Deutsche Bank AG or by its subsidiaries and/or affiliates in accordance with appropriate local legislation and regulation. For more information http://www.db.com