Fraud and Cyber Security

How to protect your organisation

BARCLAYS

Agenda

Please note that a copy of the presentation will be emailed to you.

Fundamental basics

You are the first line of defence

- Keep cyber security at the front of your mind in the war against cyber crime

Educate, educate, educate

- Cyber security is everyone's responsibility. Train all colleagues on cyber security at regular intervals, and reinforce processes

Empower your workforce

- Strong leadership and an open culture can make it easier for people to speak up and understand their role in protecting the business

Beware what you share

- Scammers research social networking channels and company websites to know when to target, and what to say

Be suspicious, and don't succumb to pressure tactics

- Fraudsters will always pile on the pressure and can spoof e-mail addresses to make them appear to be from a genuine contact, including someone from your own organisation.

Fundamental best practices

Always conduct verbal checks

Ensure details of any new or amended payment instructions (all details) are verified by using details held on file, not from the instruction.

Single points of contact

Consider setting up single points of contact with the companies you pay regularly.

Apply this same principle internally as well as externally.

Follow due diligence

Conduct audits on your accounts on a regular basis.

Staff should escalate any suspicions using single points of contact.

Types of fraud and examples

Invoice Fraud, what would you do?

- A company receives an email purporting to be from a known supplier advising a change in bank account details to an overseas account
- In line with their process, the company calls the supplier via the number provided within the email to validate the request and bank account details provided.

What happened next

- The person who answers the phone confirms both the request and payment details provided are genuine. As a result, the company makes a series of payments totalling £790,000.00 to the account
- Confirmation of Payee (CoP) are not applied as the payment type is out of scope.

Outcome

- The genuine supplier contacts the company to query non receipt of the payment due. The supplier informs them that they have not changed their bank details, and the client realises that they validated the instruction with a fraudster.

Definition

When a fraudster sends a fake invoice, or notifies your company that supplier payment details have changed, and provides alternative details in order to defraud you.

Key learn

Always conduct verbal checks using details held on file, and not those contained within the payment instruction.

Invoice Fraud, what would you do?

- A company receives an email from a known supplier advising of a change in contact details (i.e. Telephone number/point of contact/email address)
- A month later the company receives an email from the same supplier regarding an invoice, advising of a change in account details
- The company calls the supplier using contact details held on file (updated one month before).

What happened next

- The person who answers the call confirms the request and payment details as genuine, and the company makes a BACS payment for £1,394,000.00
- CoP checks were not applied as the payment type is out of scope.

Outcome

- The client uncovers the fraud when they receive a call from their relationship team advising that the receiving bank has reported the account as suspicious.

Key learn

Always conduct verbal checks on all types of communication, including the amendment of account records.

Please note that a copy of the presentation will be emailed to you.

CEO Impersonation Fraud, what would you do?

- A member of staff receives an email instruction purporting to be from a manager to make a CHAPS payment for £39,800.00 to a personal account.

What happened next

- The payment is processed and CoP checks resulted in a 'Name Match'
- No verbal checks are carried out with the manager who had requested the payment.

Outcome

- When the member of staff later queries the instruction with the manager, the manager advises that they did not send the instruction.

Definition

Also known as Business Email Compromise (BEC), fraudsters pretend to be a senior manager – often the CEO – in order to persuade an employee to make a payment.

Key learns

Conduct verbal checks and follow company policy when making payments - don't wait until its too late.

Application Fraud, what would you do?

- An application for asset finance is received by a vendor with supporting documentation in a genuine company's name, along with invoices for the asset.

What happened next

- The vendor conducts due diligence checks, but these do not include a verbal check with the application using a verified contact number
- Following this the vendor makes a Faster Payment of £90,200.00 to an account held at another bank.

Outcome

- The Fraud is discovered when the first repayment is not able to be collected, and the vendor contacts the genuine company only to find that they had not applied for the finance. As a result they take steps to review their processes to make them more robust.

Definition

When a fraudster will steal company information to apply for a line of credit in the business name, however, the funds will be paid elsewhere. This is often applied for virtually.

Key learns

Dismissing strong processes and due diligence for potential profits could result in a substantial financial loss.

Essential verbal checks

- Check receipt of request to change contact details incl. address, phone, email;
  Receipt of request to change bank details; and
  Receipt of payment request.
- Check where the request has come from
  - Internal/External request? Both need to follow the same process, without exception.
- Use details held on file to verbally check any changes with the requestor.
- Always ensure that the requestor confirms the details to you, never the other way round.

- Don't use the details which have been sent on the email/letter/invoice.
- Don't update details without checking first.

Note: Barclays may not refund any transactions that have been authorised by our clients.

Confirmation of Payee – What you need to know

Why use Confirmation of Payee?

- It enables you to confirm whether you have the correct name for the person or business you're paying, against their account details, which can help to protect against certain types of fraud.

In scope payments:

- Faster Payment Service (FPS), CHAPS and Standing Orders submitted as single payments electronically, via one of our online payment channels.

Out of scope payments:

- BACS and Currency payments.

Definition
An industry initiative designed to target Authorised Push Payment (APP) fraud in the UK, e.g. change of existing payee or impersonation fraud.

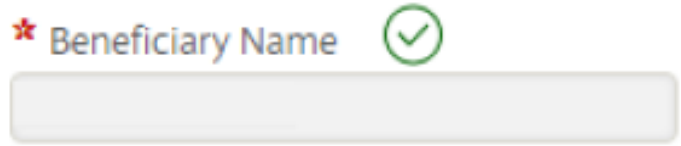
Note: This is not a silver bullet solution and should be used alongside strong internal processes including **verbal checks** with a number held on file.

Please note that a copy of the presentation will be emailed to you.

Confirmation of Payee – Indicators

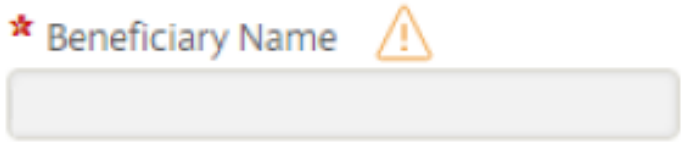
A green tick icon

- When the 'Beneficiary Name' you have entered matches the name found for that account number and sort code.



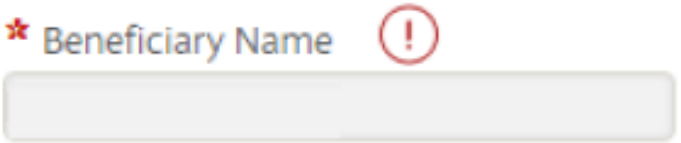
An orange warning icon

- When there is a close or partial match between the details you have provided (Beneficiary Name and Beneficiary Account Type) and those found for that account number and sort code.



A red exclamation icon

- When the Beneficiary Name does not match the name found for that account number and sort code. It is also displayed if a Beneficiary Name Validation check has not been able to take place.



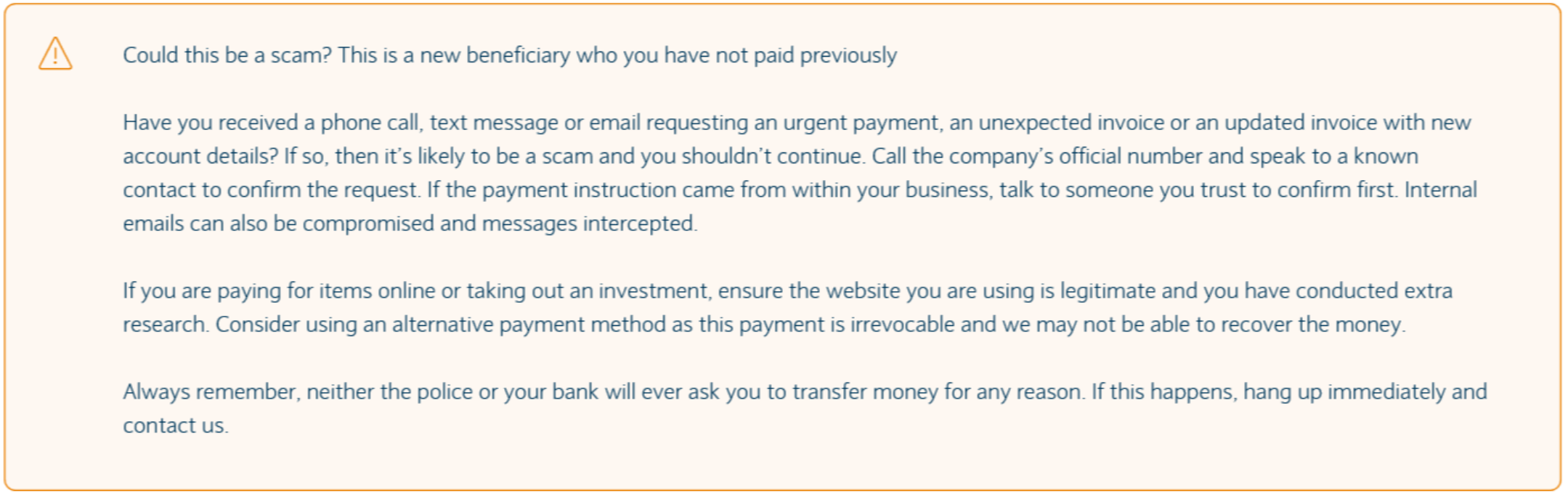
Please note that a copy of the presentation will be emailed to you.

BARCLAYS

New Beneficiary warning

When making a payment to a new beneficiary which you have not paid before using Digital Channels, the warning below will be presented.

This is your opportunity to ensure that all necessary **verbal checks** have been completed in line with your Company Policy.



Please note that a copy of the presentation will be emailed to you.

BARCLAYS

Social engineering

Social engineering – A scammer's toolkit

Sense of authority

We tend to comply with authority rather than follow our conscience.

Sense of consequence

We tend to be loss-averse and will seek to avoid a negative consequence.

Sense of urgency

We make worse decisions under stress and time pressure.

Appeal to vanity of greed

We struggle to resist opening an email attachment which promises potential rewards.

How fraudsters target you and your business

Email (Phishing)

Fraudsters pose as a legitimate source, sending emails that aim to trick people into divulging sensitive information or transferring money into other accounts.

These typically contain a link to a fake website asking for financial information, passwords or other sensitive information.

3 top tips to protect your organisation from phishing:

1. Don't click on links or open attachments from senders you are unsure of, or enter any personal or security information on a site accessed through a link in an email
2. Your bank may ask you for some information, but will never ask for your full password or PIN, provide you with details to make a payment, or request that you grant them access to your systems or PC to carry out updates, or upgrade you to a new portal
3. Consider adopting a 'Phish me/Report Phishing' add-in to your Outlook and try to have a preview option if possible.

Landline/mobile calls (Vishing) and Text Messages (Smishing)

Vishing (voice phishing) and Smishing (SMS phishing) involves receiving fraud calls or texts claiming to be from an organisation or known contact.

Common examples include the bank, the police, HMRC, a supplier or even an internal member of staff.

3 top tips to protect your business from vishing and smishing:

1. Never assume that the caller is genuine because they know information about you, your company, your colleagues, or even if they have the right caller ID
2. Fraudsters often create a sense of urgency to convince employees to act quickly without properly thinking through the implications of their actions. Always give yourself time to stop and think
3. If you're suspicious of a phone call, immediately terminate the call. To check whether it was legitimate, call a trusted contact at the organisation. Use a different phone as the fraudster can keep the original line open.

Please note that a copy of the presentation will be emailed to you.

BARCLAYS

Wider threats in the world of fraud - Malware

'Malware', short for 'malicious software', is used by criminals to disrupt computer operations and access confidential information.

Malware can be installed into your computer through clicking a link in an email, or by downloading software from a malicious source.

Ransomware

Ransomware enables a fraudster to gain control of your system to encrypt your files, demanding a fee to unlock them.

Without the decryption code, it is unlikely that you will be able to access your files again.

Trojans

Trojans enter your computer on the back of other software, acting as a back door to the computer and granting a fraudster remote access.

Once inside your device, a Trojan can give a stranger access to your personal details by taking screenshots and capturing keystrokes.

Protecting your business against malware

- Keep your firewalls and security software updated, setting updates to auto where possible.
- Install the latest updates for your internet browser and operating system.
- Only download files and software from trustworthy sources.
- Keep employees educated on how to identify phishing emails, and ensure they are aware of the initial steps to take in the event of a ransomware attack, and where to go to report fraud and scams.
- If your computer or mobile device does get infected, disconnect from the network straight away and seek professional assistance.
- Run regular security scans on your devices. Ensure you keep your important files backed up, stored off your network.
- Ensure you keep your important files backed up, stored off your network.
- Be cautious of emails or texts which ask you to follow a website link or open an attachment. Emails and texts containing malware tend to have some urgency to them.

Please note that a copy of the presentation will be emailed to you.

Wider threats in the world of fraud – Network attacks

As workforces have become more mobile, employees no longer always work on a single trusted network, making security more difficult.

It is important that sensitive information is only sent over encrypted networks. Secure Sockets Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser.

Man-in-the-Middle

In a 'Man-in-the-Middle attack' (MITM attack), the attacker intercepts the network and watches the transactions between the two parties.

They are then able to steal sensitive information, such as account passwords, banking details, or customer data.

Distributed Denial-of-Service

A Distributed Denial-of-Service (DDoS) attack is when a hacker tries to bombard a website with traffic from multiple infected sources (known as botnets), causing the site to become overwhelmed and crash.

Protecting your business against network attacks

- Use a Virtual Private Network (VPN) for remote access. VPNs add privacy and security to public networks and are used by corporations to protect sensitive data.
- In the absence of a VPN, avoid unknown public Wi-Fi sources and only use trusted secure connections.
- Websites should begin with 'https://' - the 's' stands for 'secure', however this only indicates that the link between you and the website owner is secure, and not that the site itself is authentic.
- Check the address for any subtle misspellings, additional words and characters, and other irregularities.
- Configure routers to halt more simple attacks by stopping invalid IP addresses.
- Use intrusion-detection systems (IDS), which can provide some protection against valid protocols being used against you in an attack.
- Invest in DDoS mitigation appliances, which can help to block illegitimate traffic to your website.
- Consider buying excess bandwidth that can handle spikes in demand. Alternatively, use an outsourced provider where you can buy services on demand, such as burstable circuits that provide more bandwidth when you require it.

Wider threats in the world of fraud – Money mules

The ‘money mule’ trap involves employees, often students or seasonal staff members, being offered payment in exchange for receiving money temporarily into their bank account.

They will then be asked to withdraw the cash to hand over or transfer it on.

This type of scam is on the increase, targeting students who are short of cash and may be tempted by offers to make ‘easy money’ on job search or social media websites.

Protecting your business from money mules

Raise awareness with employees who are students, and seasonal staff members - they should be wary of unsolicited approaches of ‘easy’ or ‘quick cash’ with no experience needed. If it seems too good to be true, it probably is.

Ensure that supplier details are kept up to date (Audit).

Remember the importance of **verbal checks**.

Security protocols

Security protocols – Best Practice

Smart card/SIM removal
It is recommended that you remove your smartcard/SIM from the reader once you have logged in.

Select dual approval for making transactions
Using two separate devices for set-up and authorisation.

Multi-factor authentication (MFA)?
Where the user must provide two or more pieces of evidence to verify their identity, such as:

- Fingerprint scanner (Biometric finger vein reader)
- Sign What you See (SWYS)
- Voice patterns
- Facial recognition

Regularly review latest news articles
Consider setting up notifications for service announcements in iPortal to receive regular news articles.

Strong passwords
Use upper case, lower case, numbers and special characters such as #B3Saf3!
For more information for password strategies that can help your organisation visit:
https://www.ncsc.gov.uk/collection/passwords

Please note that a copy of the presentation will be emailed to you.

Barclays Layered Security Model

Prevent:

Education & awareness

- Cyber Security Webinars
- Full Fraud Awareness Training
- Access to extensive online resources, both internal and external to Barclays.

Secure login

Barclays offers a range of security devices:

- Barclays Biometric Reader and Barclays Pinpad Reader
- Mobile Authentication – using the Barclays Corporate App
- Connectivity via USB or Bluetooth.

Digital banking controls

- Multiple Approval Levels
- Payment Limits
- Confirmation of Payee (CoP) and Beneficiary Matching.

Barclays Layered Security Model

Detect:

Fraud monitoring

- Internal tools to detect unusual or suspicious behaviour
- Software to detect Trojans and Malware
- Software to detect a Remote Access Attack based on behavioural biometrics.

Fraud payment profiling

- Monitor of outbound payment traffic
- Looking for unusual or suspicious payments
- Allows verification and confirmation with our clients to determine the validity of payments.

Recovery

- Effective Internal Recovery Department
- Global collaboration within the Industry with 24x7 contacts.

Resources and support

Fraud awareness checklist

Support

Ensure your teams have access to training and support on your financial processes.

Train

Take advantage of any training opportunities in fraud prevention and check all colleagues are aware of the latest fraud trends.

Remind

Issue regular reminders to your team on how to follow important processes and consider testing these.

Review

Test your internal prevention methods are robust and regularly reviewed.

Inform

Keep up to date with the latest information and resources. Follow your bank and Action fraud on social media to make this easier.

Protect

Ensure payments requests are input, verified and authorised following adequate internal processes and controls.

Please note that a copy of the presentation will be emailed to you.

Barclays resources

Learn more about how to protect your business from fraud by visiting our fraud and security pages online:

Fraud Protection Hub:
https://www.barclayscorporate.com/insights/fraud-protection/

Online Fraud and Cybercrime Toolkit:
https://www.barclayscorporate.com/insights/fraud-protection/cyber-fraud-toolkit/

Security, Digital Channels Help Centre:
https://www.barclayscorporate.com/digitalchannels/digital-channels-help-centre/security.html

Follow us on social media:

- **Twitter** - @BarclaysCorp
- **LinkedIn** - Barclays Corporate Banking

Please note that a copy of the presentation will be emailed to you.

BARCLAYS

Barclays fraud support

If you fall victim to fraud where payments have been sent via Barclays.net, BACS or File Gateway, call the Barclays Online Fraud Helpdesk immediately on:

- **0800 056 4890 (opt 2)** if calling from within the UK
- **(+44) 0330 156 0155 (opt 2)** if calling from within the UK

Both lines are open 24/7.

To report fraud or any suspicious activity for all other products, including Business Online Banking, call Barclays UK Fraud Operations on:

- **0345 050 4585** (open 24/7)

To maintain a quality service we may monitor or record phone calls.

Report any suspicious emails purporting to be from Barclays to **internetsecurity@barclays.co.uk**

Additional reporting routes

- Forward text messages (Smishing) free of charge to **7726**
- Forward non Barclays Phishing emails to the Email Reporting Service (SERS) report@phishing.gov.uk
- Fraudulent attacks, even if unsuccessful, should be reported to Action Fraud by calling:

  0300 123 2040

  Or visiting: actionfraud.police.uk

Other resources

The National Cyber Security Centre (NCSC)

Supporting the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public:
www.ncsc.gov.uk

Fraud Advisory Panel: Love Business. Hate Fraud.

We're proud to be partnering with the Fraud Advisory Panel to help and support businesses in the fight against fraud:
www.lovebusiness-hatefraud.org.uk

Please note that a copy of the presentation will be emailed to you.

BARCLAYS

Questions?

BARCLAYS

Disclaimer:

This document has been prepared by Barclays Bank PLC and is provided to you for information purposes only and may be subsequently amended, superseded or replaced.

Every attempt has been made to ensure that the information provided is accurate. However, neither Barclays Bank PLC ("Barclays") nor any of its employees makes any representation or warranty (express or implied) in relation to the accuracy, reliability or completeness of any information or assumptions on which this document may be based and cannot be held responsible for any errors. No liability is accepted by Barclays (or any of its affiliates) for any loss (whether direct or indirect) arising from the use of the information provided.

Please note that a copy of the presentation will be emailed to you.