Cyber fraud

Protecting your business against the current threats
Contents

3 Introduction
4 Social engineering
5 Invoice fraud
6 CEO fraud
7 Phishing
8 Vishing and smishing
9 Malware
11 Network attacks
12 Distributed denial-of-service attack
14 Conclusion
15 Further guidance and resources
16 About the author
Falling victim to a cyber fraud attack can result in major financial losses, while data breaches can severely damage customers’ trust in a company. Fraudsters can easily monetise stolen information by selling it online, and the impact of this on businesses’ reputations can be severe. Individuals have been given increased anonymity as internet and email-based transactions have become the norm in business. Fraud, more than ever, may cover many different jurisdictions, with victims, beneficiaries and fraudsters potentially located in different countries. This makes it difficult to investigate fraud and, crucially, very hard to recover funds. For this reason, businesses must look to prevent fraud, rather than hope to cure its consequences.

At Barclays, we are dedicated to helping you protect your business from the risks of cyber fraud attacks. This document aims to outline some of the key cyber fraud threats your business may face today, and offer guidance on how to mitigate those risks. We can’t cover every fraud risk your business may be exposed to in a single document, so this guidance is intended as a supplement to your own fraud risk management.
Social engineering

The threat of cyber fraud can seem difficult to combat, as the software used by fraudsters can be extremely complex. However, it is important to remember that most cyber fraud attacks depend heavily on human interactions — fraudsters have long identified that the easiest way to breach an organisation’s defences is to target its people, not its systems.

Social engineering is the method by which fraudsters aim to trick people into breaking normal security procedures. Fraudsters are usually looking for the victim to give up sensitive information, such as bank login details, or for them to enable malicious software to be installed onto their device. They may also trick the victim into carrying out a fraudulent payment themselves.

Fraudsters in social engineering cases often have thorough knowledge of the company to enable them to build trust with the victim. They may be aware of regular payments that are due, or of the structure of teams within your company, enabling them to impersonate internal employees.

The most common forms of social engineering for business customers are:

• Invoice fraud
• CEO
• Phishing
• Vishing
• Smishing

When you receive a request to make a payment always take five seconds to stop and ask yourself if this feels right.

Information loss is the largest cost component for organisations, representing 43% of costs in 2017

Accenture, 2017

4/5 of the top causes of data breaches are because of human error

Information Commissioner’s Office (ICO), Data security incident trends, 2018
Invoice fraud involves a fraudster notifying your company that supplier payment details have changed and providing alternative details in order to defraud you.

Invoice fraudsters are often aware of the relationships between companies and their suppliers, and will know the details of when regular payments are due. The fraud may only be discovered when the legitimate supplier follows up on non-payments.

Fraudulent letters and emails sent to companies are often well-written, meaning the fraud is difficult to spot without strong operating processes and controls in place. Email addresses are easy to spoof, or in the case of malware-infected PCs, criminals can access genuine email addresses.

The process of changing the bank details of someone you are paying should always be treated with extreme caution.

### Protecting your business against invoice fraud

- Always verify details of any new / amended payment instructions verbally by using details held on file, and not on the instruction. Fraudsters can spoof email addresses to make them appear to be from a genuine contact, including someone from your own organisation.
- If you are suspicious about a request made by phone, ask the caller if you can call them back on a trusted number. Fraudsters will attempt to pressure you into making mistakes — take the pressure off by taking control of the situation.
- Consider removing information such as testimonials from your own or your suppliers’ websites or social media channels that could lead fraudsters to knowing who your suppliers are.
- Look carefully at every invoice and compare it to previous invoices received that you know to be genuine — particularly the bank account details, wording used and the company logo.
- Consider setting up single points of contact with the companies you pay regularly.
- Apply the same principles to requests from within your own organisation.
- Electronic payments in the UK are made based on sort code and account number only, and any account name given is not routinely checked, therefore independent verification is important.
- Regularly conduct audits on your accounts.
- Make all staff aware of this type of fraud, particularly those that are responsible for making payments.

### Case study

A company in the property sector was required to pay their supplier over £102,000 at the end of the month. Not long before the payment was due, they received a message advising of a change of account details. The payment was duly made to the new account as instructed. A week later, the genuine supplier called to ask why they had not received their funds. As a week had passed, there was now only £300 left in the account used by the fraudsters — the rest had been withdrawn and spent. Consequently, the company’s bank were unable to recover the funds.
CEO fraud

CEO fraud, also known as Business Email Compromise (BEC) or CEO impersonation fraud, occurs when fraudsters pretend to be a senior manager — often the CEO — in order to persuade a staff member to make a payment.

This fraud is a request, often made via email, purporting to come from a senior person in the company, normally to the accounts department, requesting an urgent payment to a supplier or partner.

The fraud attempt sometimes occurs when the senior person is out of the office, and the request may outline that the transaction is confidential and sensitive in order to discourage further verification.

For instance, the fraudster may try to convince the victim that their company is about to acquire another business, and the payment is needed as a down-payment for the confidential deal.

Protecting your business against CEO fraud

- Any payment requests with new or amended bank details received by email, letter or phone should be independently verified. This includes internal emails from senior management that contain payment requests. Fraudsters can spoof email addresses to make them appear to be from a genuine contact, including someone from your own organisation
- Don’t be pressured by urgent requests, even if they appear to originate from someone senior — remember this is a common tactic adopted by fraudsters
- Be cautious of how much information you reveal about your company and key officials via social media platforms and out-of-office automatic replies
- Consider removing information such as testimonials from your own or your suppliers’ websites or social media channels that could lead fraudsters to knowing who your suppliers are
- Regularly conduct audits on your accounts
- Make all staff aware of this type of fraud, particularly those that make payments

Case study

A client received an email purporting to be from the Financial Director instructing that 50% of an invoice be paid to an account. The payment of £75k required approval and was held for security checks by Barclays’ fraud prevention team.

When contacted by Barclays, the client confirmed the payment was genuine and it was released.

The client then received a second email which appeared to be genuinely from the Financial Director requesting the remaining 50% be paid to a different bank account. This payment was not held for any security checks.

The fraud was discovered when the genuine beneficiary reported that they had not received their payment. The client informed them of the bank accounts they had paid, and the supplier advised that the accounts did not belong to them.

It was not the client’s policy to verbally confirm payment instructions of this type as it appeared to be an internal email. The client believes that the email account belonging to the Financial Director had been compromised and reported it to their IT department for further investigation.

The fraudsters had moved the money before the alarm was raised, leaving only a small amount available for recovery.
Phishing involves a fraudster, posing as a legitimate source, sending emails or letters that aim to trick people into divulging sensitive information or transferring money into other accounts. The emails typically contain a link to a fake website, which will request that you enter financial information. Alternatively, emails may contain an attachment in the form of a document, form or notification.

Alternatively, emails may contain an attachment in the form of a document, form or notification. Equally, the email may be designed to contain and deliver malware via an attachment or a link. If the link is clicked or the attachment opened, the criminal will be able to gain access to your system.

Protecting your company against phishing

- Be alert to the style, tone and grammar of emails you receive, especially if the email doesn’t address you by name (e.g. “Dear Sir / Madam”)
- Never enter any personal or security information on a site accessed through a link in an email
- Never click on links or open attachments from senders you are unsure of
- On sites that require you to input sensitive information, look for ‘https’ in the website address — the ‘s’ stands for ‘secure’, though be aware that this does not guarantee the website is genuine
- Do not assume a sender is genuine because they know information about you / your company or the email address looks familiar — fraudsters are skilled in collecting enough information and can spoof email addresses to make them appear to be from a genuine contact, including someone from your own organisation
- Remember that Barclays 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
- If you receive a suspicious email purporting to be from Barclays, forward it to internetsecurity@barclays.co.uk then delete it straight away
- Make all staff aware of this type of fraud, particularly those that make payments

Case study

Employees of a client received an email appearing to be from their employer asking them to log into their ‘secure portal’ in order to find out what their annual bonus figure would be. The email contained a link leading to a fake portal which looked like the genuine one, which duped employees into thinking they were logging on securely. Fraudsters were able to capture the log in credentials of each employee who entered them on the fake portal.

Following this, the fraudsters were able to use these details to log in to the genuine secure portal, and change the employee’s bank details, so that earnings were paid into the fraudster’s account and transferred away.

30% of phishing emails get opened by targeted users and 12% of those click on the attachment or link

Verizon Data Breach Investigations Report, 2018
Vishing and smishing

Vishing (voice phishing) and smishing (SMS phishing) involves fraudsters calling or texting purporting to be from the police, utility providers, delivery companies or even your bank.

They may claim that your account has been compromised, suspicious activity on the account, or that a payment has been made by the business using incorrect bank details. Caller IDs or numbers on display are relatively easy to change or spoof. Fraudsters have been known to convince people a call is genuine by getting them to cross-check the incoming call number with the official number of the bank, however fraudsters can use technology to spoof numbers which make them appear to be coming from a genuine source.

Smishing is similar — but is carried out through SMS text message. The text often contains a phone number, which connects you to the fraudster. As with vishing, details can be spoofed, so it can seem as if the texts are coming from a legitimate source and they can even be inserted into genuine text communications with the bank.

Protecting your business against vishing and smishing

- Do not assume a caller is genuine because they know information about you or your company — fraudsters are skilled in collecting enough information to sound convincing and can change caller display IDs to a genuine number
- If you are suspicious, terminate the call and call back using your usual contact number, and not one provided by the caller
- Remember that your bank may ask you for some information, but will never ask for your full password or PIN, payment authorisation codes, provide you with details to make a payment, or request that you grant them access to your systems or PC
- We will never text clients a link that leads to the online banking log-in page, or to ask for confirmation of account or security details
- Make all staff aware of this type of fraud, particularly those that make payments

Case study

The client received a call from a male claiming to be from Barclays. The caller’s number appeared on the client’s display as a genuine Barclays number. The caller advised the client to use the online phone number checker to verify the call is genuinely from Barclays.

The caller told the client that their account had been accessed from a suspicious location. The caller advised the client that they would need to block all of their accounts, this would need to be done manually, by sending payments with an unusual reference. A total of 9 payments, totalling £156k were made by the client following these instructions.

Barclays’ fraud prevention team identified the unusual beneficiary names and references on four of the payments which were held, and called the customer to ask for further details.

During the call with the client it became apparent that they were also on the other line to someone from the fraudster impersonating Barclays. The client was informed of how vishing scams work and they were advised to hang up on the other caller.

Initially the client was confused and did not know who to believe. Barclays provided relevant information so that the client could independently verify the genuine call and be confident they were speaking to Barclays.

Fortunately, on this occasion this scam was averted due to the unusual reference used and the banks internal fraud detection systems, but fraudsters have been known to be so convincing that clients have disregarded the banks advice, and demanded that payments are released.

43% of businesses and 19% of charities experienced a cyber-security breach or attack in the last 12 months

Cyber Security Breaches Survey, Gov.uk, 2018
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, opening an attachment to an email, or by downloading software from a malicious source.

Trojans

Trojan programs are a type of malware that enter your computer on the back of other software. They act as back doors to the computer, granting a fraudster remote access. Once inside your device, a trojan can give a stranger access to your personal details by taking screenshots or capturing keystrokes.

When logging into online banking websites, an unexpected screen might appear, delaying you or asking you to repeatedly input data. While you are delayed by these, a fraudster could be setting up another payment elsewhere, waiting for you to unwittingly authorise it by inputting your PIN.

Trojans are hard to detect as they remain passive when not in use. Firewalls and anti-virus software help to defend against trojans, but can’t guarantee your protection. You should always be cautious of ‘pop-ups’ on your screen requesting that you put your card into the reader, input your PIN, or allow a download.

Ransomware

Ransomware enables a fraudster to gain control of your system in order to encrypt your files, demanding a fee to unlock them. Without the decryption code, it is very unlikely that you will be able to access your files again.

Though in many cases the criminals will restore files when the ransom is paid, there is no guarantee this will be the case. Hackers have been known to share stolen private customer information free of charge on the web in order to punish a company for not paying their proposed ransom.

When logging into online banking websites, an unexpected screen might appear, delaying you or repeatedly input data. While you are delayed by these, a fraudster could be setting up another payment elsewhere, waiting for you to unwittingly authorise it by inputting your PIN.

Ransomware attacks take on average 23 days to resolve

Accenture, 2017

Cryptomining

Cryptocurrency mining, commonly known as ‘cryptomining’ or ‘cryptojacking’, is a type of malware which is rapidly becoming a major threat for businesses. Cryptomining is when a fraudster infects a PC, server, smartphone or IoT connected device with malware, and uses the processing power to mine for cryptocurrency.

The increase in cryptomining attacks has occurred due to the rapid rise in value in recent months of cryptocurrencies, such as Bitcoin. Cryptomining is an easy, low-risk way for fraudsters to make money, meaning that these attacks are likely to continue to grow.

Currently, detection of cryptomining is very difficult due to the breadth of the activity. The most obvious effect of a cryptomining attack is that businesses may experience some availability issues and a slowdown in responses from their servers. However, cryptomining attacks are designed to avoid detection and cause the least possible disruption, making the attacks difficult for businesses to notice.

Malware attacks cost companies $2.4m on average

Accenture, 2017

Ransomware attacks take on average 23 days to resolve

Accenture, 2017

Cryptomining

Cryptocurrency mining, commonly known as ‘cryptomining’ or ‘cryptojacking’, is a type of malware which is rapidly becoming a major threat for businesses. Cryptomining is when a fraudster infects a PC, server, smartphone or IoT connected device with malware, and uses the processing power to mine for cryptocurrency.

The increase in cryptomining attacks has occurred due to the rapid rise in value in recent months of cryptocurrencies, such as Bitcoin. Cryptomining is an easy, low-risk way for fraudsters to make money, meaning that these attacks are likely to continue to grow.

Currently, detection of cryptomining is very difficult due to the breadth of the activity. The most obvious effect of a cryptomining attack is that businesses may experience some availability issues and a slowdown in responses from their servers. However, cryptomining attacks are designed to avoid detection and cause the least possible disruption, making the attacks difficult for businesses to notice.

Malware attacks cost companies $2.4m on average

Accenture, 2017

Ransomware attacks take on average 23 days to resolve

Accenture, 2017

Cryptomining

Cryptocurrency mining, commonly known as ‘cryptomining’ or ‘cryptojacking’, is a type of malware which is rapidly becoming a major threat for businesses. Cryptomining is when a fraudster infects a PC, server, smartphone or IoT connected device with malware, and uses the processing power to mine for cryptocurrency.

The increase in cryptomining attacks has occurred due to the rapid rise in value in recent months of cryptocurrencies, such as Bitcoin. Cryptomining is an easy, low-risk way for fraudsters to make money, meaning that these attacks are likely to continue to grow.

Currently, detection of cryptomining is very difficult due to the breadth of the activity. The most obvious effect of a cryptomining attack is that businesses may experience some availability issues and a slowdown in responses from their servers. However, cryptomining attacks are designed to avoid detection and cause the least possible disruption, making the attacks difficult for businesses to notice.
Protecting your business against malware

Device security
- 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
- Be cautious of emails which ask you to follow a website link or open an attachment
- Run regular security scans on your devices
- Ensure you keep your important files backed up, stored off your network
- If your computer does get infected, disconnect from the network straight away and seek professional assistance

Online banking
- If you have a smart card, never leave it in the reader connected to your computer
- If possible, select dual approval for making transactions, using two separate machines for setting up this authorisation
- Be wary about pop-ups for PINsentry resets when logging into online banking (your PINsentry will never need updating or resetting)
- Never remake payments to alternative account details if asked to do so
- Never enter your PIN in order to allow a download
- Never re-enter your PIN at login or while making a payment
- If you notice anything unusual on your online banking screens, abandon your banking session and tell Barclays at once

Case study
A member of staff at an SME opened an email and clicked on a link that contained malware. The malware infected the computer system and encrypted all the files so that no access could be gained by members of staff. The criminals contacted the company, giving them 24 hours to pay £2,000 in bitcoin to unlock their system. The company had not backed up their files, so was particularly vulnerable. The company contacted Action Fraud, who advised them not to pay the ransom. They were then able to restore their machines, but unfortunately lost some important files due to not being fully backed up.

“Malware is usually effective because it targets vulnerabilities in systems which have not been updated. It is essential that antivirus software is deployed and that systems are patched regularly to ensure the latest security updates are installed. The damage done by malware can also be reduced by making frequent backups of data which are then stored securely in a separate system or place.”

DCI Andrew Gould
Operation Falcon, Metropolitan Police Service
As workforces have become more mobile, employees no longer always work on a single trusted network, making security more difficult.

Emails are the main communication method for most companies, yet it is often forgotten how unsecure the communications are. An email can be thought of like a postcard — it can be read as it moves across networks.

It is therefore 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 attack**

There are various different types of network attack, but all require the exploitation of an unsecured network. Where the network is not encrypted, an unknown third party may intercept communications that are being sent. In a ‘Man-in-the-middle 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.

A common example of a Man-in-the-Middle Attack is ‘active eavesdropping’. This is when the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.
Protecting your business against network attacks

A distributed denial-of-service attack (DDoS attack) is when a hacker tries to bombard a website with traffic from multiple sources, causing the site to become overwhelmed and crash. Attackers create a network of infected computers known as botnets by sending and spreading malware through websites, emails and social media.

Once the malware has been distributed it allows the hacker to launch an attack remotely, sometimes using a botnet of over a million different users, without their knowledge.

There are places on the Dark Web where it is possible to buy and sell botnets or individual DDoS attacks. For a small fee, a fraudster can disrupt an organisation’s online operations, causing them to lose out on sales and suffer from damage to their reputation.

The most sustained DDoS attack lasted 297 hours (12.4 days), the longest in recent years.
Kaspersky Lab Q1 2018 DDoS Intelligence Report

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
- On sites that require you to input sensitive information, look for ‘https’ at the beginning of the website URL — the ‘s’ stands for ‘secure’
- Ensure there is a padlock symbol in the URL address bar — this shows that your connection is secure
- 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
Distributed denial-of-service attack (cont.)

- **Attacker**
- **Controller**
- **Zombies**
- **Victim**
Opportunities for cyberattacks are sure to grow in the coming years, with McAfee’s predictions forecasting a vast increase in cyber usage.

Being stringent about cybersecurity can fall by the wayside when running a business — the return on investment is difficult to quantify, as success lies in the avoidance of loss. Ensuring that your company has good cyber hygiene will help to keep you safe from fraudsters.

**Keep your software updated**

Investing in up-to-date cyber-defence software is imperative to protecting your business from the financial and reputational consequences of cyber fraud. You should also ensure that your internet browsers are updated to the most recent versions. Testing your own controls to ensure they are operating as appropriate will also enable you to identify system weaknesses before fraudsters get to exploit them. Always ensure that important files are backed up to a removable hard drive disk or to the cloud.

**Your people are a weakness and a defence**

Raising awareness of fraud within your company is key to its prevention. Ensuring that employees who can authorise payments are aware of potential threats will lessen your chances of a cyber fraud attack succeeding.

It is important to create a culture in your company where employees are encouraged to report fraud threats, so they do not feel they need to hide a breach they may have been unwittingly involved in.

Please share our fraud awareness videos with your payment teams — these can be found at barclayscorporate.com/fraudawareness
Further guidance

If you have any queries, please speak to your Relationship Director.

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

0800 056 4890
(if calling from within the UK) or

+44 (0) 330 156 0155
(if calling from outside the UK) (both open 24/7).

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

0345 050 4585
(open 24/7).

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

Fraudulent attacks, even if unsuccessful, should be reported to Action Fraud by calling

0300 123 2040
or visiting

actionfraud.police.uk

If you receive a suspicious email that appears to be from Barclays, please forward it to

internetsecurity@barclays.co.uk
and then delete it from your email account immediately.

Learn more about how to protect your business from fraud at our fraud smart centre

barclayscorporate.com/fraudawareness

Further resources

• actionfraud.police.uk
• barclayscorporate.com/fraudawareness
• consilium.europa.eu
• getsafeonline.org
• gov.uk
About the author

Ben Chance
Barclaycard
International, Fraud
Transaction Cycle Lead

Ben joined Barclays in October 2018 as the Global Head of Global Fraud Operations reporting to Karoline Kane. He is responsible for the Fraud Transaction Cycle.

Ben joined Barclays from Goldman Sachs in New York, where he spent the last three years as the head of Fraud Strategy and Business Risk Officer for the Marcus Digital Finance business. While with Goldman, he built an integrated end to end fraud program for the consumer businesses and ensured appropriate operational and regulatory risk management throughout the design, build, and operational stages of multiple newly formed business units.

Prior to joining Goldman Sachs, Ben was with Capital One for twelve years. He held various leadership roles in US Card across Operations Analysis, Process Engineering, Branded Card Fraud and Disputes, as well as Partnerships Card Fraud and Disputes. Ben joined Capital One after seven years as an active duty submarine officer in the US Navy. He holds a MBA from the University of Virginia Darden School of Business and a BS in Marine Engineering from the United States Naval Academy.

Ben is based in Whippany New Jersey, he and his wife Jennifer have three children ages 16, 15 and 12.

barclayscorporate.com