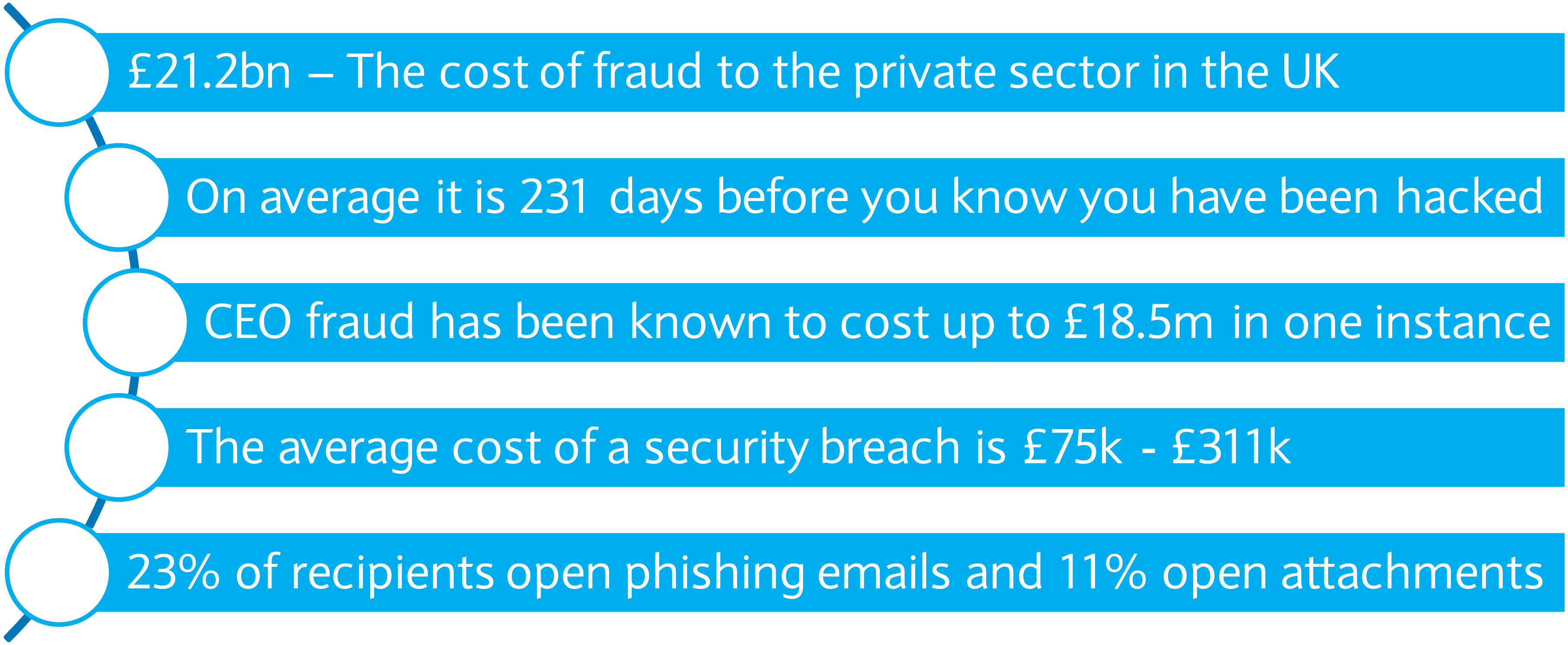
BARCLAYS

Know your cyber and fraud risks

Agenda

- Overview of cybercrime
- The top cyber threats to UK Businesses and how to remain safe
- Current fraud threats
- Payment security
- What help is available
- Further reading

Setting the scene



£21.2bn – The cost of fraud to the private sector in the UK

On average it is 231 days before you know you have been hacked

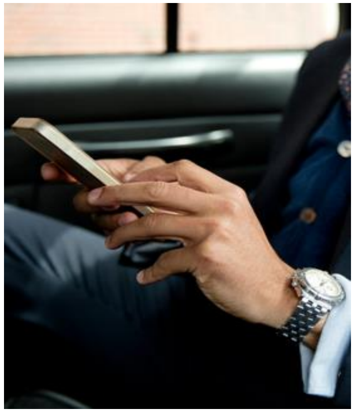
CEO fraud has been known to cost up to £18.5m in one instance

The average cost of a security breach is £75k - £311k

23% of recipients open phishing emails and 11% open attachments

Sources:
http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-digital.pdf - Relates to points 2&4
https://londondsc.co.uk/ - Relates to points 1 & 5
https://www.cert.gov.uk/ - Relates to all points
Data Breach investigations Report - Relates to point 5   Action fraud – relates to point 3

Social engineering



Social engineering is one of the most prolific and effective means of gaining access to secure systems and obtaining sensitive information, yet requires minimal technical knowledge. Your people are your biggest weakness when it comes to cyber security.

“The manipulation of situations and people that result in the targeted individuals divulging confidential information”

CIFAS fraud prevention agency

The scammer’s toolkit

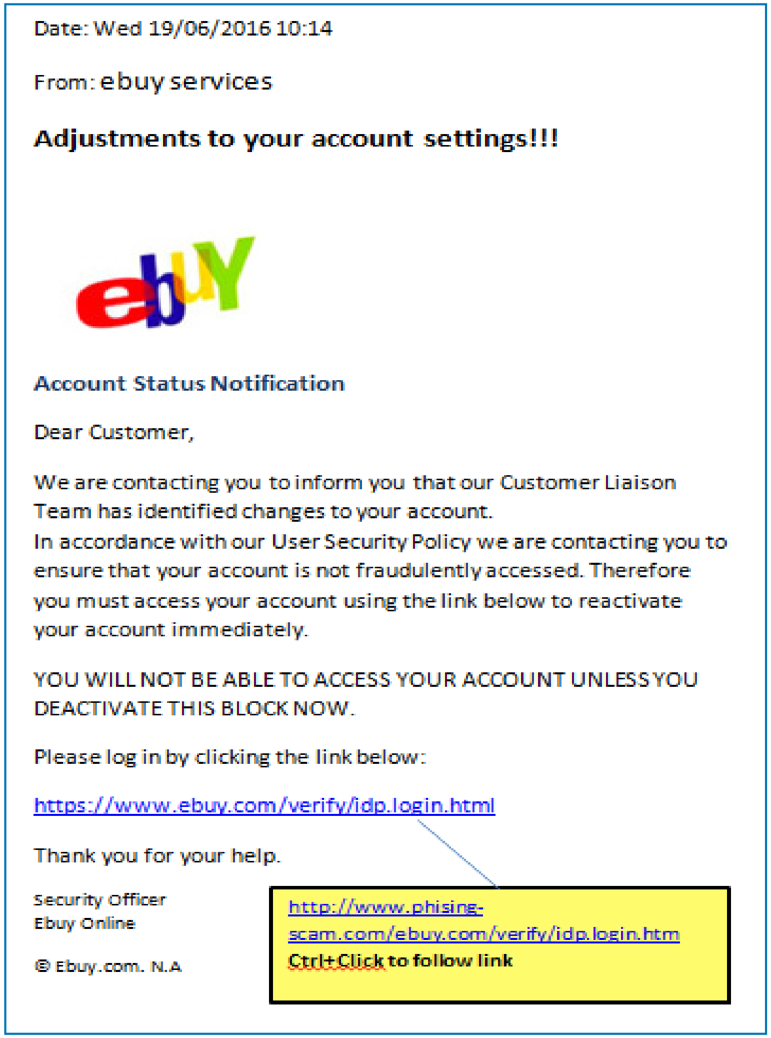
Create a sense of authority
We tend to comply with authority rather than follow our conscience.

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

Create a sense of urgency
We make worse decisions under stress and time pressure

Appeal to our vanity or greed
We struggle to resist opening that email attachment which promises to tell us how much our colleagues get paid.

Phishing/spear email – what to look for



Date: Wed 19/06/2016 10:14

From: ebuy services

Adjustments to your account settings!!!

Account Status Notification

Dear Customer,

We are contacting you to inform you that our Customer Liaison Team has identified changes to your account.
In accordance with our User Security Policy we are contacting you to ensure that your account is not fraudulently accessed. Therefore you must access your account using the link below to reactivate your account immediately.

YOU WILL NOT BE ABLE TO ACCESS YOUR ACCOUNT UNLESS YOU DEACTIVATE THIS BLOCK NOW.

Please log in by clicking the link below:

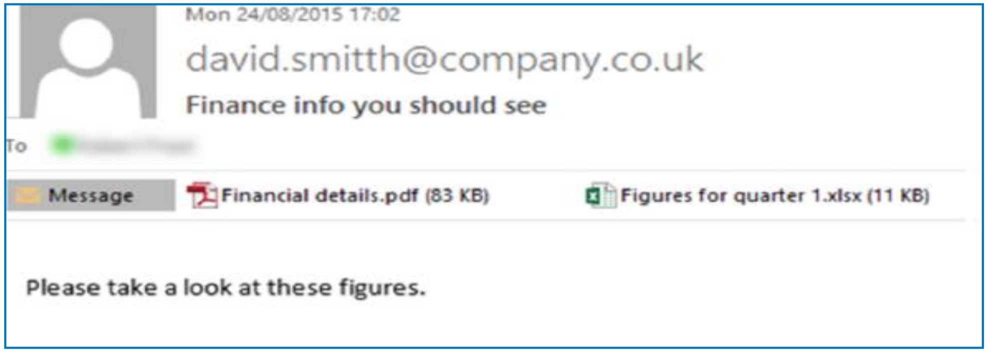
https://www.ebuy.com/verify/idp.login.html

Thank you for your help.

Security Officer
Ebuy Online

® Ebuy.com. N.A

http://www.phising-scam.com/ebuy.com/verify/idp.login.htm
Ctrl+Click to follow link



Mon 24/08/2015 17:02

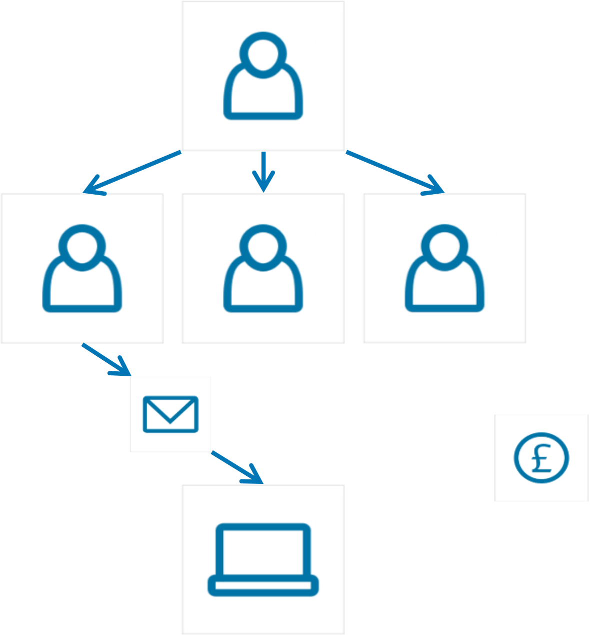
david.smitth@company.co.uk

Finance info you should see

To [redacted]

Message | Financial details.pdf (83 KB) | Figures for quarter 1.xlsx (11 KB)

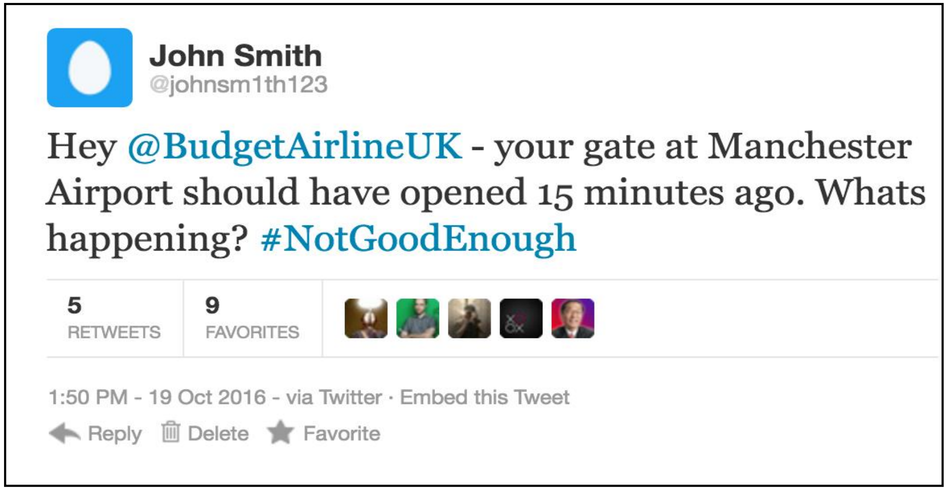
Please take a look at these figures.



Social engineering

Sometimes the information we post onto social media can appear harmless and innocent, but it can often be used by cyber criminals to form part of an attack.

What information can we learn about someone from the post opposite? How could this information be used against us?



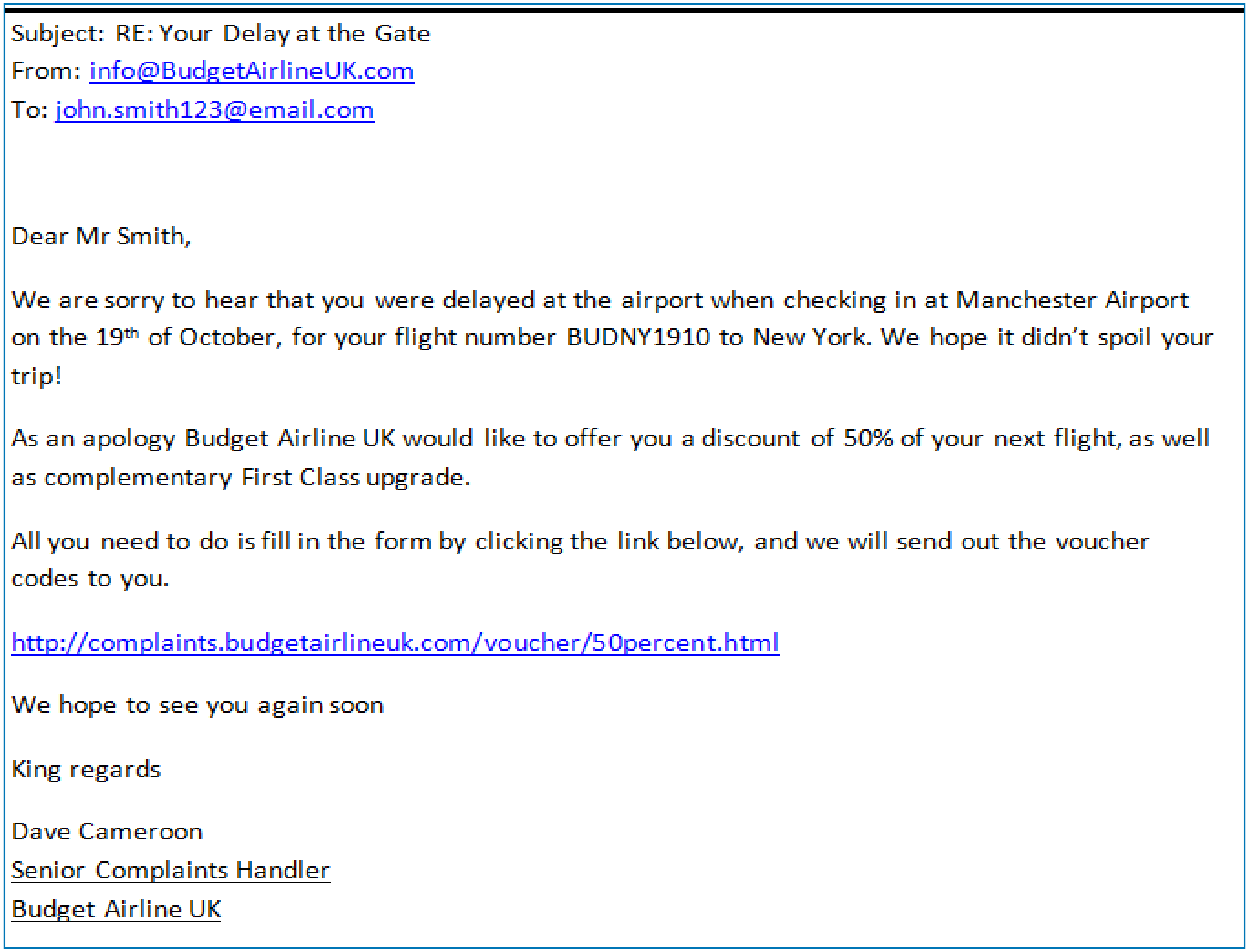
John Smith
@johnsm1th123

Hey @BudgetAirlineUK - your gate at Manchester Airport should have opened 15 minutes ago. Whats happening? #NotGoodEnough

5 RETWEETS 9 FAVORITES

1:50 PM - 19 Oct 2016 - via Twitter · Embed this Tweet

Social engineering



Subject: RE: Your Delay at the Gate
From: info@BudgetAirlineUK.com
To: john.smith123@email.com

Dear Mr Smith,

We are sorry to hear that you were delayed at the airport when checking in at Manchester Airport on the 19th of October, for your flight number BUDNY1910 to New York. We hope it didn't spoil your trip!

As an apology Budget Airline UK would like to offer you a discount of 50% of your next flight, as well as complementary First Class upgrade.

All you need to do is fill in the form by clicking the link below, and we will send out the voucher codes to you.

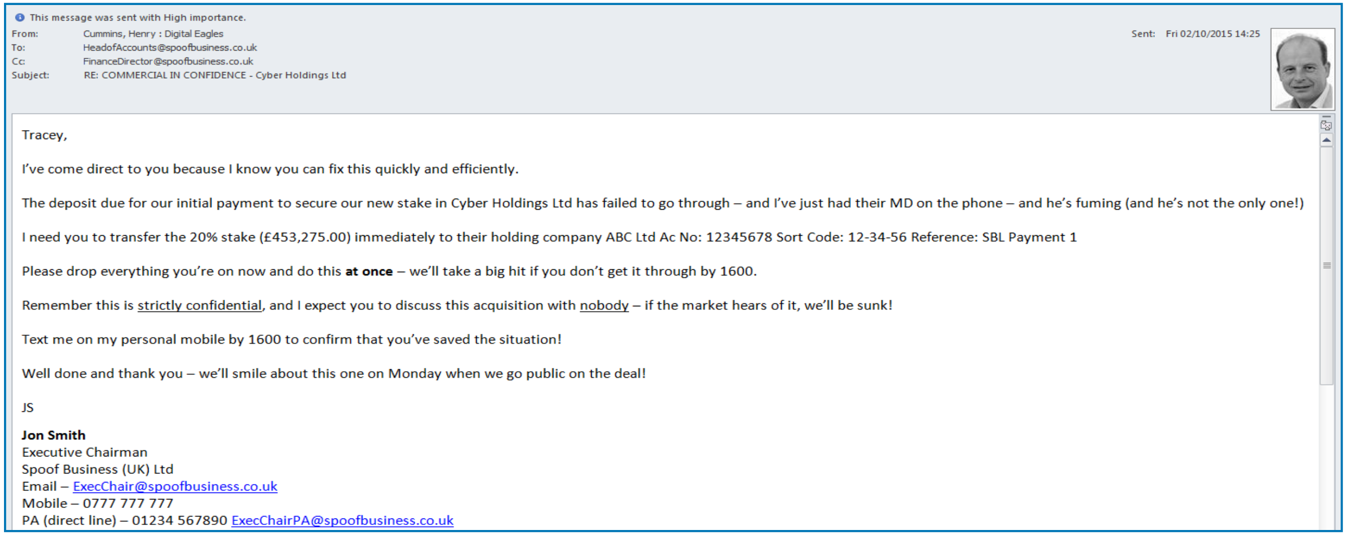
http://complaints.budgetairlineuk.com/voucher/50percent.html

We hope to see you again soon

King regards

Dave Cameroon
Senior Complaints Handler
Budget Airline UK

CEO impersonation fraud



This message was sent with High importance.

From: Cummins, Henry : Digital Eagles

To: HeadofAccounts@spoofbusiness.co.uk

Cc: FinanceDirector@spoofbusiness.co.uk

Subject: RE: COMMERCIAL IN CONFIDENCE - Cyber Holdings Ltd

Sent: Fri 02/10/2015 14:25

Tracey,

I've come direct to you because I know you can fix this quickly and efficiently.

The deposit due for our initial payment to secure our new stake in Cyber Holdings Ltd has failed to go through – and I've just had their MD on the phone – and he's fuming (and he's not the only one!)

I need you to transfer the 20% stake (£453,275.00) immediately to their holding company ABC Ltd Ac No: 12345678 Sort Code: 12-34-56 Reference: SBL Payment 1

Please drop everything you're on now and do this **at once** – we'll take a big hit if you don't get it through by 1600.

Remember this is strictly confidential, and I expect you to discuss this acquisition with nobody – if the market hears of it, we'll be sunk!

Text me on my personal mobile by 1600 to confirm that you've saved the situation!

Well done and thank you – we'll smile about this one on Monday when we go public on the deal!

JS

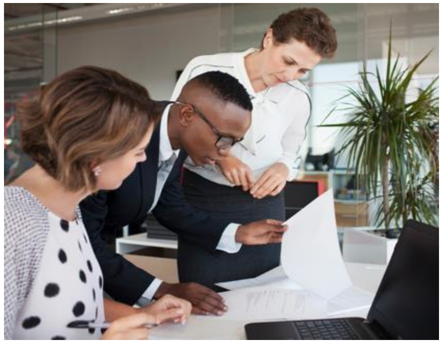
Jon Smith
Executive Chairman
Spoof Business (UK) Ltd
Email – ExecChair@spoofbusiness.co.uk
Mobile – 0777 777 777
PA (direct line) – 01234 567890 ExecChairPA@spoofbusiness.co.uk

- CEO fraud is when a fraudster hacks a CEO or a senior employee's personal or corporate email account and send an email requesting a payment to an account which the fraudster is in control of
- Fake email addresses can also be created which are similar to that of the CEO or senior official, and fraudsters can disguise emails as being sent by the recognised sender
- They can insert fake emails into existing genuine email trails.

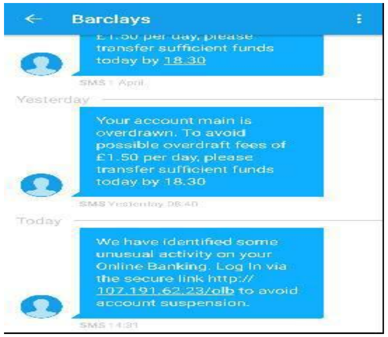
To help protect your organisation

- Be cautious about any unexpected emails which request bank transfers, even if the message appears to have originated from someone within your organisation and is how your business usually operates
- Always check payment requests directly with the member of staff using details held on file to confirm the instruction is genuine.

Examples of social engineering



Supplying details to a fraudster who has phoned you claiming to be from your bank or credit card provider. They advise you that your account has been compromised and that you need to transfer money to a ‘safe’, ‘holding’ or ‘cloud account’ to protect it. They may even know information about your account such as balances or transactions to convince you they’re genuine. This is known as **vishing.** Caller ID can also be manipulated to trick you that calls are coming from a known number.



Barclays

£1.50 per day, please transfer sufficient funds today by 18.30

SMS 1 April

Yesterday

Your account main is overdrawn. To avoid possible overdraft fees of £1.50 per day, please transfer sufficient funds today by 18.30

SMS Yesterday 08:40

Today

We have identified some unusual activity on your Online Banking. Log In via the secure link http://107.191.62.23/olb to avoid account suspension.

SMS 14:31

Text messaging scams called **SMishing** – these occur when you receive a text message that appears to be from your bank and often shows up in the same message feed, asking you to confirm or supply account information. This is especially dangerous since many of us receive genuine text messages from our banks.

Mobile bugs – This year has seen the introduction of mobile malware that has become considerably more sophisticated than what’s been there before. A common theme is the attempt to root the phone in order to provide complete control and a establish a permanent presence on the device.

How to avoid social engineering attacks

- Never reveal personal or financial data including usernames, passwords, PINs, or ID numbers. Remember that a bank or other reputable organisations will never ask you for this information or to move your money – whether by email, call or SMS
- Do not assume a caller is genuine because they have some basic information about your account and don't trust caller ID – it can be manipulated to display a genuine looking number
- Do not allow remote access to Barclays.net – Barclays will never ask for this
- If you receive such a call, hang up and call the Barclays.net fraud team using official contact details held on file
- Do not open email attachments from unknown sources
- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.

Cyber attack – start point

Malware gives the fraudster access to personal information, account details, passwords, key logging and mouse movement, ability to watch the victim's screen. Trojans often open 'backdoors' to the affected computer system, giving the fraudster remote access.

- Removable storage
- Embedded documents
- Links and downloads
- Virus-infected networks.

Passwords are the front door keys to an organisation, and here is how to get hold of them:

- Deception – tricking you into revealing it
- Brute force – an automated effort to hack your password
- Spyware – recording your login
- Shoulder surfing – watching you log in.

The most commonly used passwords of 2016

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321
11. qwertyuiop
12. mynoob
13. 123321
14. 666666
15. 18atcskd2w
16. 7777777
17. 1q2w3e4r
18. 654321
19. 555555
20. 3rjs1la7qe
21. google
22. 1q2w3e4r5t
23. 123qwe
24. zxcvbnm
25. 1q2w3e

*Source: Keep Security

Banking trojans

There are trojan viruses in circulation such as ‘dridex’ which can grant a cyber criminal access to your bank accounts.

- You get a message to update your smart card reader software
- You are prompted to enter your card number and pin to start the download
- A trojan downloads, takes control of the computer and starts to steal your money.

Note:

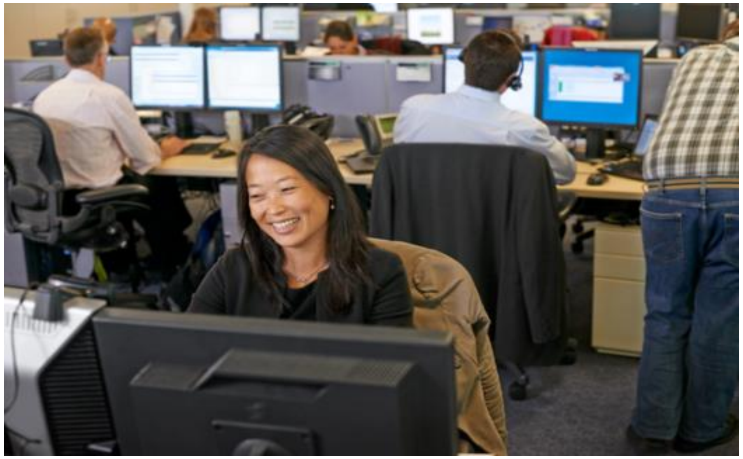
- Be wary of offers of automatic updates or additional verification steps
- Never enter your card number or PIN other than when logging in, authorising a payment or approving an administrative change.

If this happens:

- Remove your smart card immediately
- Disconnect the infected machine from the network
- Contact us for additional support on 0330 1560155 (+44 1606 566 208). *Calls to 03 numbers use free plan minutes if available; otherwise they cost the same as calls to 01/02 prefix numbers. Calls may be monitored or recorded in order to maintain high levels of security and quality of service*

Malware

A new threat is emerging where fraudsters are using malware to remotely access accounts packages to edit stored beneficiary details. By editing the beneficiary account details, fraudsters are able to redirect regular payments.



Be aware of what is happening

Step 1: Fraudsters use malware to remotely access your accounts package and edit existing beneficiaries. They then wait for you to complete the below steps

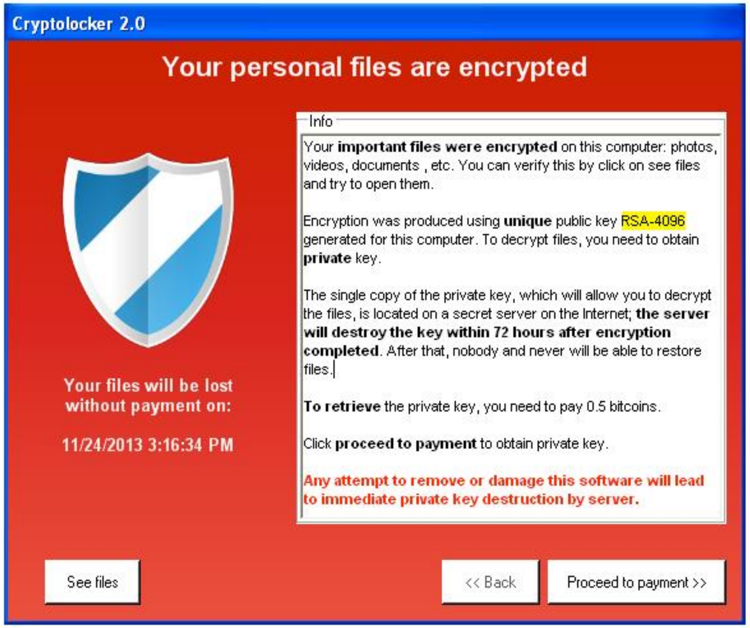
Step 2: A supplier or salary run is initiated in the accounts package by a genuine user to pay legitimate invoices or salaries

Step 3: The payment file is created by the accounts package, now using the amended account details of known beneficiaries

Step 4: A genuine user then imports the file and authorises the payments, only checking the file total rather than checking the beneficiary account information.

Ransomware

Ransomware is a form of malicious software (malware) that gives cyber criminals the ability to lock a computer from a remote location. A pop-up window is displayed informing the owner that it will only be unlocked once a sum of money is paid. Experts warn that ransomware is the fastest growing form of computer malware.



Your personal files are encrypted

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Things to consider

- Do you regularly back up your data, including to a USB connected device stored remotely from your computer?
- Do you have anti-virus/antispyware software and firewall running?

Common types of attack

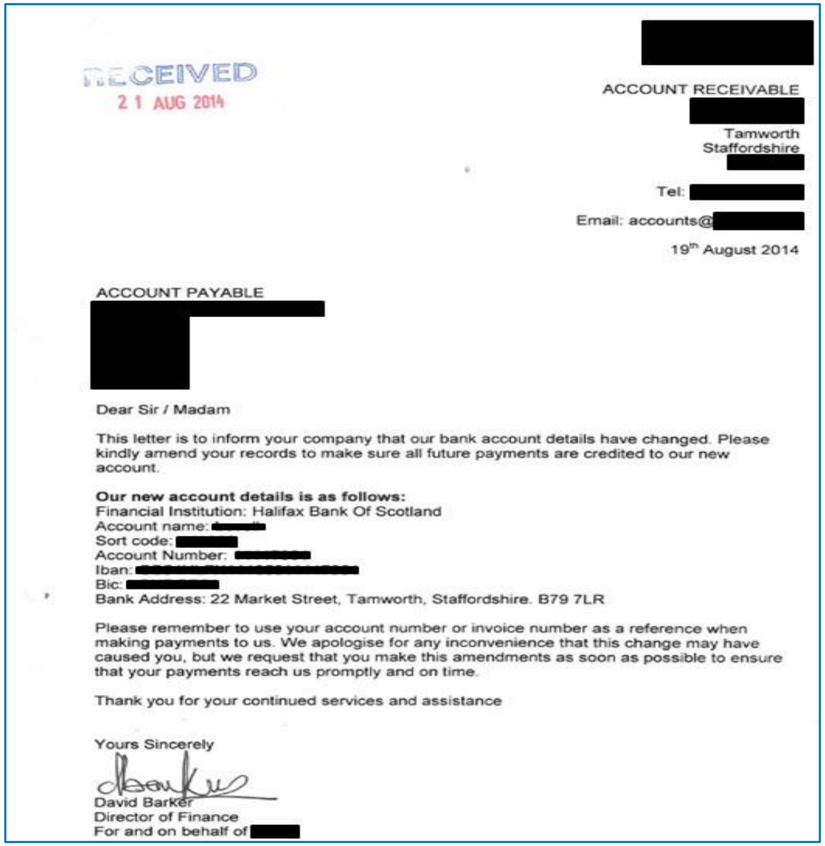
Man in the middle attack

The attacker intercepts the network and watches the transactions between the two parties and steals sensitive information. Consider using a Virtual Private Network when connecting to public Wi-Fi.

DDoS attack

Overwhelming your servers to take your site down and deny service to your site/servers.

Invoice fraud



[redacted]

RECEIVED
21 AUG 2014

ACCOUNT RECEIVABLE
[redacted]
Tamworth
Staffordshire
[redacted]

Tel: [redacted]

Email: accounts@[redacted]

19th August 2014

ACCOUNT PAYABLE
[redacted]

Dear Sir / Madam

This letter is to inform your company that our bank account details have changed. Please kindly amend your records to make sure all future payments are credited to our new account.

Our new account details is as follows:
Financial Institution: Halifax Bank Of Scotland
Account name: [redacted]
Sort code: [redacted]
Account Number: [redacted]
Iban: [redacted]
Bic: [redacted]
Bank Address: 22 Market Street, Tamworth, Staffordshire. B79 7LR

Please remember to use your account number or invoice number as a reference when making payments to us. We apologise for any inconvenience that this change may have caused you, but we request that you make this amendments as soon as possible to ensure that your payments reach us promptly and on time.

Thank you for your continued services and assistance

Yours Sincerely

David Barker
Director of Finance
For and on behalf of [redacted]

- Invoice fraud is when a fraudster sends an instruction purporting to be from a known or new supplier or customer advising of a change of or new bank details, which the fraudsters control
- The instruction will be by email, telephone or letter.

To help protect your organisation

- Make all staff aware and always call your supplier or client, using contact details you have on file, to confirm any change in bank details
- Please remember that electronic payments in the UK are made based on sort code and account number only. Any account name given is not routinely checked. This is the same for all UK banks and it is the responsibility of the remitter to ensure the account details being used are correct by conducting independent verification.

Barclays ring-fence and the fraud risks

To help protect your organisation

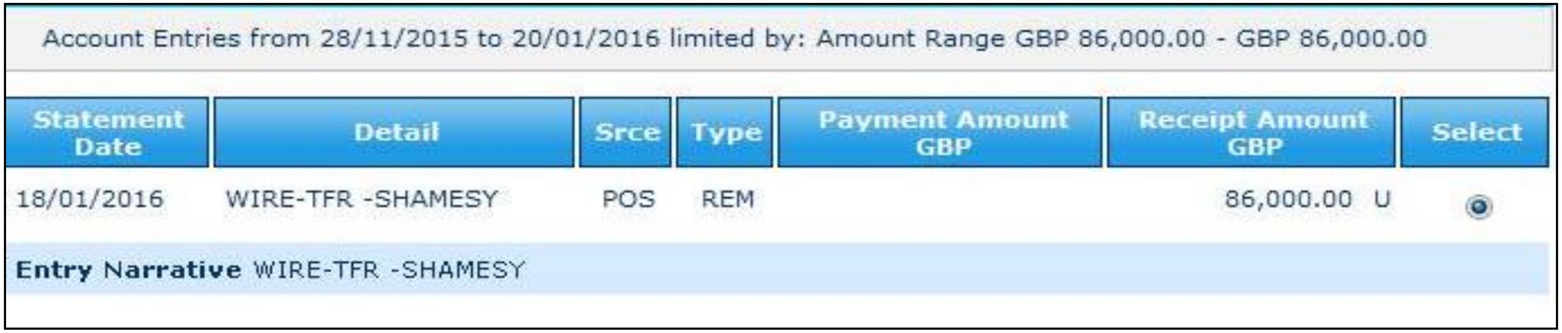
- From time to time Barclays will send e-mails containing links. If you are suspicious or you feel the e-mail is unsolicited you can contact us via your usual channel or report the email to internetsecurity@barclays.co.uk
- Barclays will not make requests for payments or security details via email or any other communication
- Barclays is only changing sort codes – account numbers remain the same; however, other banks going through this process may also be changing account numbers
- Any payment requests with new bank details received by email, letter or phone must be independently verified using contact details held on file. This includes internal emails from senior management which contain payment requests
- Electronic payments in the UK are made based on sort code and account number only and any account name given is not routinely checked. Clients must ensure the account details being used are correct by conducting independent verification
- To watch a fraud awareness video and further guidance, visit www.barclayscorporate.com/fraudawareness

Cheque overpayment fraud

- Fraudsters issue a cheque either unexpectedly, or for services or goods provided at an amount higher than owed, and then request that the overpayment is refunded to them
- The client is duped into paying the refund on the assumption that the cheque has cleared or will clear, but it bounces leaving the client out of pocket.

To help protect your organisation

- Don't be fooled by the narrative – fraudsters are entering things like Bacs or CHAPS into these boxes, so at a glance, the payment doesn't look like a cheque
- Be sure the funds are cleared before you deliver goods or services and never pay any refunds against **uncleared** funds
- If in doubt, speak to your relationship team
- To find out how you can customise your Barclays.Net balance summary page to view the 'cleared/un-cleared' status of funds, please login to Barclays.Net and view the "Reporting: Cash Statements Guide" under the Help Section.



Account Entries from 28/11/2015 to 20/01/2016 limited by: Amount Range GBP 86,000.00 - GBP 86,000.00

Statement Date	Detail	Srce	Type	Payment Amount GBP	Receipt Amount GBP	Select
18/01/2016	WIRE-TFR -SHAMESY	POS	REM		86,000.00 U	◉

Entry Narrative WIRE-TFR -SHAMESY

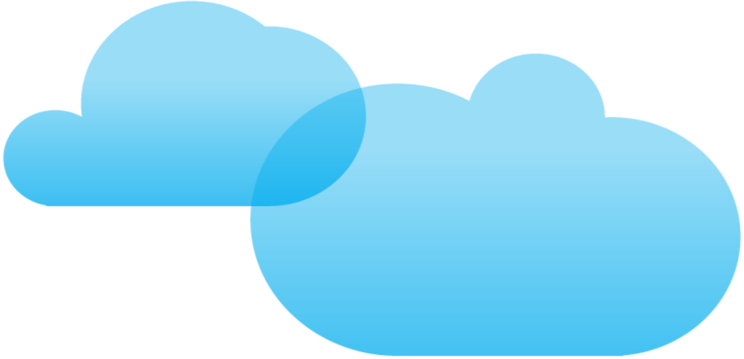
Security in the cloud

Questions to ask yourself

Are you backing up or storing?

Where is the data located? Different countries have different data protection laws

What are the policies of the service providers to recover data etc?



Is your data segmented or compartmentalised in the cloud?

Does the provider have malware protection?

Who owns the data once in the cloud?

10 steps to cyber security

Some basic guidance

User Education and Awareness
Educate all your employees no matter what their level or role

Network Security
Avoid connecting to untrusted networks

Monitoring
Constantly monitor inbound and outbound traffic

Malware Protection
Ensure you have the most update version of your chosen software

Information Risk Management
Embed an Information Risk Management Regime across your organisation

Incident Management
Establish an incident response and disaster recovery plan

Managing User privileges
Do they need the access?

Secure Configuration
Remove or disable unnecessary functionality

Home and Mobile Working
Protect data using an appropriately configured Virtual Private Network

Removable media Controls
Limit removable devices such as USB drives

“Please note that the following information is not a comprehensive guide to cyber security and keeping yours and your customers information safe. There can be no replacement for having the expertise of a cyber security professional and regular testing of systems and networks. We always recommend seeking out professional expertise to ensure you are compliant with all legalities and requirements from a data protection perspective.”

Payment security

	Cost	Ease	Risk mitigation
Use strong passwords and change default ones	£	⚙	✓ ✓ ✓
Protect your card data and only store what you need	£	⚙	✓ ✓
Inspect payment terminals for tampering	£	⚙	✓ ✓
Install patches from your vendors	£	⚙ ⚙	✓ ✓ ✓
Use trusted business vendors and know how to contact them	£	⚙	✓
Protect in-house access to your card data	£	⚙ ⚙	✓ ✓
Don’t give hackers easy access to your systems	£ £	⚙ ⚙	✓ ✓ ✓
Use anti virus software	£ £	⚙ ⚙	✓ ✓
Scan for vulnerabilities and fix issues	£ £	⚙ ⚙	✓ ✓ ✓
Use secure payment services solutions	£ £ £	⚙ ⚙	✓ ✓ ✓
Protect your business from the internet	£ £	⚙ ⚙ ⚙	✓ ✓ ✓
For the best protection make your data useless to criminals	£ £ £	⚙ ⚙ ⚙	✓ ✓ ✓

These security basics are organised from easiest and least cost to implement to those that are more complex and costly to implement. The amount of risk reduction that each provides to small merchants is also indicated in the “Risk Mitigation”

Source – Payment Card Industry Security Standards Council -www.pcisecuritystandards.org/pci_security/small_merchant

Internet security software

- Nothing guarantees 100% security – but up to date Anti-Virus software makes you a more difficult target
- Barclays.Net customers can get free WebRoot security software.

What support is available

National Cyber Security Centre
a part of GCHQ

The National Cyber Security Centre (NCSC) will bring the UK's cyber expertise together to transform how the UK tackles cyber security issues.

Formerly CERT-UK which was the national computer emergency response team working towards enhancing the UK's cyber resilience.

CiSP
A CATALYST FOR COLLABORATION

NCSC hosts the Cyber Security Information Sharing Partnership (CiSP) which is a joint industry/government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business. When signing up you will find a regional group to join that can help you get started.

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

A nationally recognised certification establishing that you take cyber security seriously and have stood up to resilience checks carried out by a professional body.

UK customer and clients cyber crime reporting

Clients If you have been a victim of cybercrime or fraud, you should report it to the authorities. This action will not only confirm an incident has occurred, but will also help them in the days and weeks that follow an attack.

Where to report cybercrime and fraud
In the UK report all fraud and cybercrime allegations to Action Fraud:
Online: www.actionfraud.police.uk
Telephone: 0300 123 2040

Unless:

- A crime is in progress or about to be committed
- There is a locally known suspect can be easily identified
- The crime involves a vulnerable victim

If any of these are the case contact the police directly on 999, or 101 if not an emergency.

You can also report to your local police station.

Met Police: Little Book of Cyber Crime/Little Book of Big Scams
Since 2016 Barclays has been sponsoring the Met Police's two booklets on scams. The booklets are designed to offer small and medium businesses guidance on how to stay safe in the cyber world. These booklets are available to view and download from the Internet.

Customer and client reporting to Barclays
You can report Barclays phishing emails, fake Barclays websites and social media profiles for investigation by sending the information onto: internetsecurity@barclays.com

The Barclays promise

Barclays will contact customers from time-to-time but will never:

- Ask you to reveal your PIN
- Ask you to change your PIN
- Ask you for your password
- Send unsolicited requests to download software
- Ask for your smart card number, except in response to a call from you to resolve a specific issue
- Call and ask a client to make a payment
- Provide bank details to a client to make payments
- Ask a client to allow access to their system. If the client receives such a call they should act with caution and contact their relationship team immediately to verify.

Always take time to validate any such request to ensure that the person making the request is who they say they are and has the required authority.

Avoid replying to emails, take care when clicking on any links or opening attachments, and be careful when calling back taking care to use independently obtained contact details.

Barclays' services are secure

Online and mobile banking both have multiple layers of protection:

- Data sent between you and Barclays is encrypted securely
- You have secure access to our online channels
- We have advanced fraud detection processes.

Remember to:

- Use a PIN pad
- Remove the card after login – and keep it secure
- Two to sign – use configurable signing and authorisation controls.

Further reading

- digital.wings.uk.barclays – our platform to educate all staff members in all things digital. Please log on and complete the cyber security module to enhance your understanding
- www.cyberaware.gov.uk – HM Government site – Be Cyber Aware is a cross-government campaign funded by the National Cyber Security Programme
- www.cyberaware.gov.uk/cyberessentials – Cyber Essentials – Government-backed and industry supported scheme to guide businesses in protecting themselves against cyber threats
- ncsc.gov.uk – working with partners across industry, government and academia to enhance the UK’s cyber resilience
- actionfraud.police.uk In the UK report all fraud and cybercrime allegations to Action Fraud:Telephone: 0300 123 2040
- www.barclayscorporate.com/fraudawareness – a list of videos explaining the types of social engineering fraud used by cyber criminals
- getsafeonline.org – an online resource of advice about staying safe while online
- pcisecuritystandards.org/pci_security/small_merchant – information for small merchants
- http://www.met.police.uk/docs/little_book_scam.pdf - general scam and cyber crime information

Thank you

Disclaimer

Barclays offers corporate banking products and services to its clients through Barclays Bank PLC. This presentation has been prepared by Barclays Bank PLC ("Barclays"). This presentation is for discussion purposes only, and shall not constitute any offer to sell or the solicitation of any offer to buy any security, provide any underwriting commitment, or make any offer of financing on the part of Barclays, nor is it intended to give rise to any legal relationship between Barclays and you or any other person, nor is it a recommendation to buy any securities or enter into any transaction or financing. Customers must consult their own regulatory, legal, tax, accounting and other advisers prior to making a determination as to whether to purchase any product, enter into any transaction of financing or invest in any securities to which this presentation relates. Any pricing in this presentation is indicative. Although the statements of fact in this presentation have been obtained from and are based upon sources that Barclays believes to be reliable, Barclays does not guarantee their accuracy or completeness. All opinions and estimates included in this presentation constitute the Barclays' judgment as of the date of this presentation and are subject to change without notice. Any modelling or back testing data contained in this presentation is not intended to be a statement as to future performance. Past performance is no guarantee of future returns. No representation is made by Barclays as to the reasonableness of the assumptions made within or the accuracy or completeness of any models contained herein.
Neither Barclays, nor any officer or employee thereof, accepts any liability whatsoever for any direct or consequential losses arising from any use of this presentation or the information contained herein, or out of the use of or reliance on any information or data set out herein.

Barclays and its respective officers, directors, partners and employees, including persons involved in the preparation or issuance of this presentation, may from time to time act as manager, co-manager or underwriter of a public offering or otherwise deal in, hold or act as market-makers or advisers, brokers or commercial and/or investment bankers in relation to any securities or related derivatives which are identical or similar to any securities or derivatives referred to in this presentation.

Barclays Bank PLC is a member of the London Stock Exchange.

Barclays is a trading name of Barclays Bank PLC and its subsidiaries. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register No. 122702). Registered in England. Registered number is 1026167 with registered office at 1 Churchill Place, London E14 5HP.