Know your cyber and fraud risks

March 2019

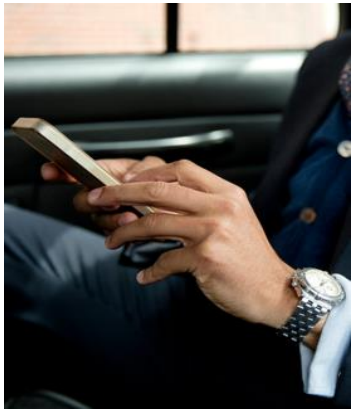
Setting the scene

- Financial fraud losses across payments, cards, remote banking and cheques totalled £768.8 Million in 2016
- On average it is 231 days before you know you have been hacked
- 46 % of UK Businesses overall identified cyber security breaches or attacks in the last 12 months
- 72% of breaches related to staff receiving fraudulent email

Sources:

https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/fraud_the_facts.pdf - Relates to point 1
https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/FFA_Annual_Review_2017_WEB.pdf - Relates to point 2
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609187/Cyber_Security_Breaches_Survey_2017_inforgraphic_general_business_findings.pdf - Relates to pints 3 & 4

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:

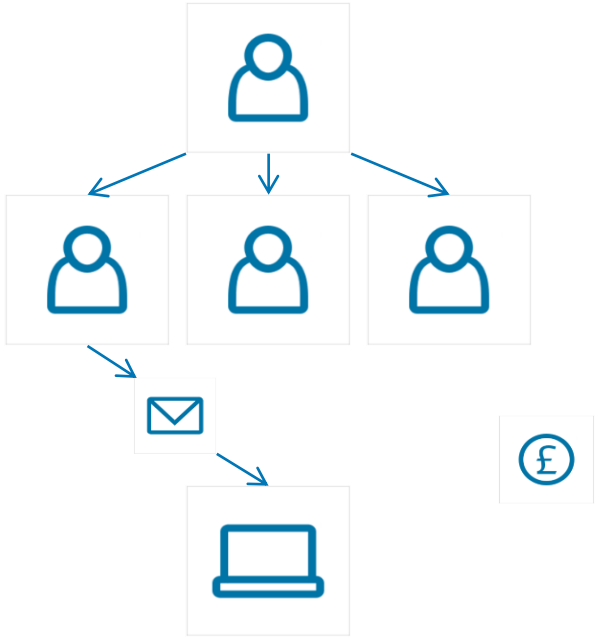
https://www.ebuy.com/verify/idp.login.html

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



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?

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

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

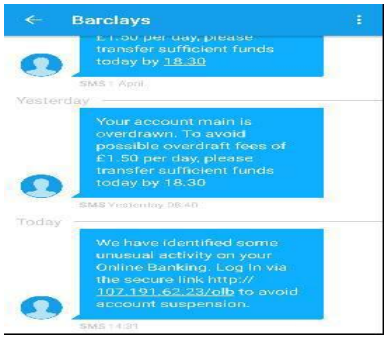
- CEO fraud is when a fraudster hacks a CEO , senior employee's, or agents personal or corporate email account and send an email requesting a payment to an account which the fraudster is in control of
- Fake email addresses can also be created which are similar to that of the CEO or senior official, 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.



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.

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.

Passwords – How secure are yours?

Top 10 Passwords of 2017*

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou

Passwords and the Internet of Things

Connected devices:

- Security Cameras
- Watches
- Thermostat
- Lights
- Routers

Have you changed the default passwords?

If you haven't you could be giving hackers the keys to your network!

*Source: fortune.com/2017/12/10/the-25-most-used-hacked-passwords-2017-starwars-freedom/

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.

ATM Fraud

- There are 2 main types of ATM Fraud, Distraction Scam and Keyboard Logging
- Distraction Scam involves 2/3 fraudsters, one distracting you by saying you have dropped money on floor, second/third keep an eye on what the PIN you have typed is and swaps your genuine card with a fake
- Keyboard loggers usually are placed in remote ATM locations such as 24/7 supermarkets
- When coming up to ATM beware of a loose keyboard/card insert and any pin holes in the place directly above the pin pad.

Courier Fraud

- Interesting and clever scam created by fraudsters targeting vulnerable people
- Originally Fraudster will contact customer to say card has been used for Fraud and new card will be sent
- Next day a courier will arrive at door with ‘new card’ but will ask to identify customer by entering PIN into ‘security device’
- Once PIN is confirmed, courier will hand ‘new card’ to customer while removing ‘fraudulent card’
- What actually has happened is card is fine but with the PIN entered into the ‘security device’, fraudster has access to card and PIN to go on to online banking and start to transfer all funds out

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 business banking products and services to its clients through Barclays Bank UK PLC. This presentation has been prepared by Barclays Bank UK 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 UK PLC is a member of the London Stock Exchange.

Barclays is a trading name of Barclays Bank UK PLC and its subsidiaries. Barclays Bank UK 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.