BARCLAYS

Cyber Security

November 2016

Regional Digital Eagles

Agenda

- Overview of Cyber Crime
- The top cyber threats to UK businesses and how to remain safe
- 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've been hacked
- 74% of small businesses suffered a security breach last year
- 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 2,3 &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

BARCLAYS

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*

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:

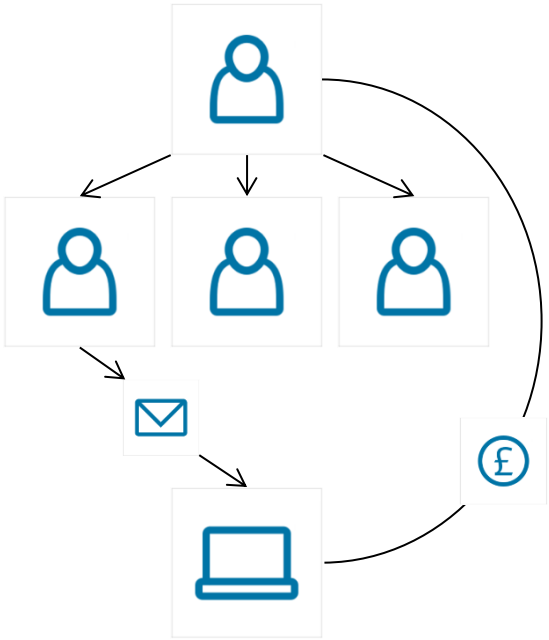
https://www.ebuy.com/verify/idp.login.html

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



BARCLAYS

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?

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

Examples of Social Engineering

Supplying details to a fraudster who has phoned you claiming to be from your bank or credit card provider, or from the police and telling you there is a problem. They ask you to confirm confidential information in order to solve the problem. This is known as **vishing.** They may even dispatch a 'Courier' to collect payment cards or other records from you, known as courier fraud.

Text messaging scams called **SMiShing** – short for SMS phishing – are very similar to traditional phishing except they happen via text message versus email. In a typical scam, you would receive a text message that appears to be from your financial institution and often shows up in the same message feed, asking you to confirm or supply account information. This is especially dangerous since some of us are used to receiving official 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 devise.

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.
- Be very careful that people or organisations to whom you are supplying payment card information are genuine, and then never reveal passwords. Remember that a bank or other reputable organisations will never ask you for your password, pins or authentication codes via email, phone call or SMS
- 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 Points

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 log in.
- Shoulder surfing – watching you log in.

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).

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 window is then displayed informing the owner that it will only be unlocked once a sum of money is paid. Ransomware is the fastest growing form of computer malware , experts warn.

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

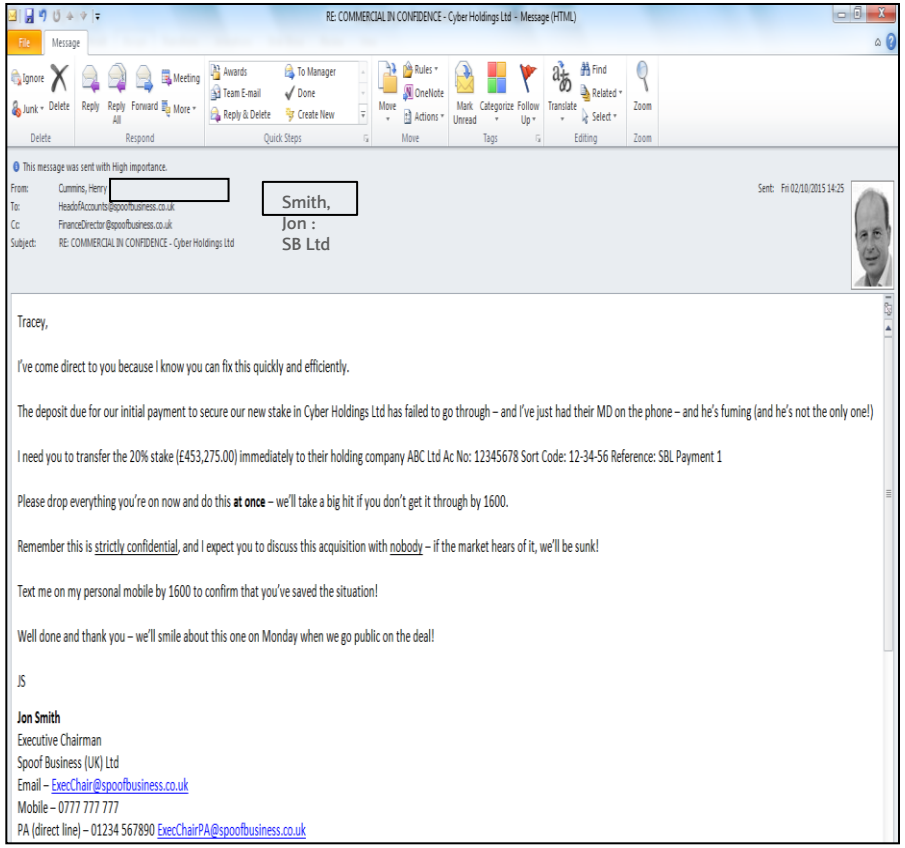
Man In the Middle Attack

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.

Common types of attack



RE: COMMERCIAL IN CONFIDENCE - Cyber Holdings Ltd - Message (HTML)

This message was sent with High importance.

From: Cummins, Henry [redacted]
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

Smith,
Jon :
SB Ltd

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

Claiming that you need to change your payment destination or a demand for payment via phone, fax and email.

RECEIVED
21 AUG 2014

[redacted]
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

Claiming that you need to change your payment destination or a demand for payment via phone, fax and email.

Fraud smart tips – Cheques – receiving

- Be alert to unexplained or unexpected credits to your account
- Be sure the funds are cleared before you deliver goods or provide services
- Don't be fooled by the narrative it does not mean the funds are cleared
- Never pay any refunds to somebody against **uncleared** funds
- If in doubt speak to your relationship team
- Also find guidance on cheques and clearing timescales at http://www.chequeandcredit.co.uk/cheque_and_credit_clearing/the_cheque_clearing_cycle

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

Future trends

1bn more computer users in next 4 years

400% increase in data being stored in next 5 years

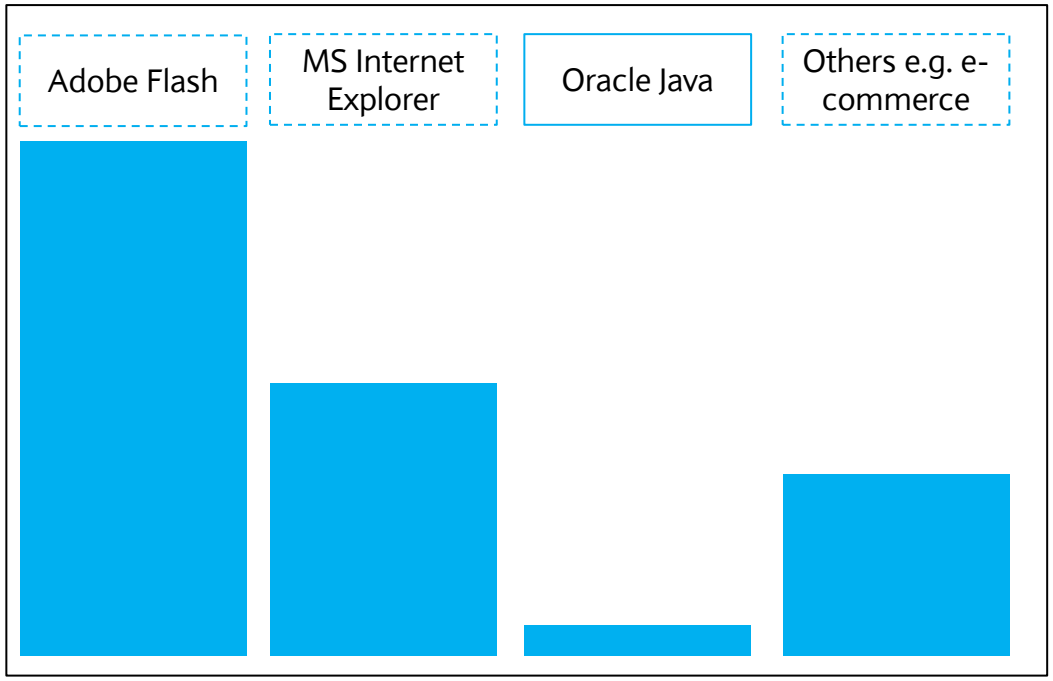
2.6bn increase in smartphone connections in next 5 years

580 million extra smart watch users in next 3 years

In 2016 there will be a large increase in the theft and sale of data from payment systems with over 760 crypto currencies now available.

2016 will be the year of Exploitation with Ransomware increasing inline with the growth of crypto currencies.

Vulnerabilities by Application



The current risk with e-commerce lies in the software for the shopping baskets. If this is not updated it can become vulnerable.

Source: Mcafee

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."Credit CESG

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 it makes you a more difficult target.
- Barclays Online Banking customers can get free Kaspersky security software.
- BIB and barclays.net customers can get free WebRoot security software.

What support is available

CERT-UK

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

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.

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.

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
- cyberstreetwise.com - HM Government site – Be Cyber Streetwise is a cross-government campaign funded by the National Cyber Security Programme
- cyberstreetwise.com/cyberessentials - Cyber Essentials – new 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 - The UK's national fraud and internet crime reporting centre
- barclayscorporate.com/information/fraud-videos.html - 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

Thank you