Cyber Security

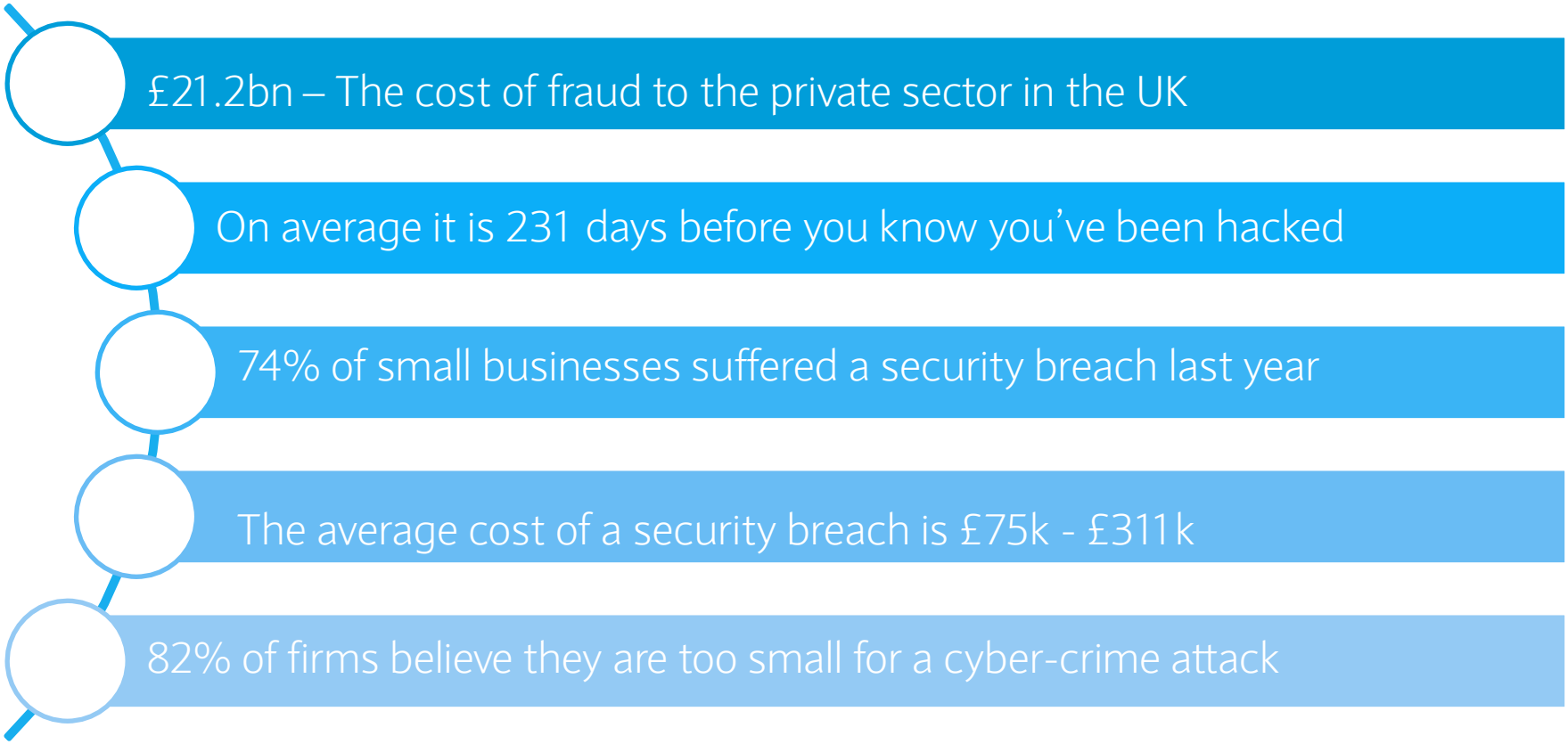
February - 2016

BARCLAYS

Agenda

- Overview of Cyber Crime
- The top cyber threats to UK businesses and how to remain safe
- What help is available
- Further reading

Setting the scene



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 point 5

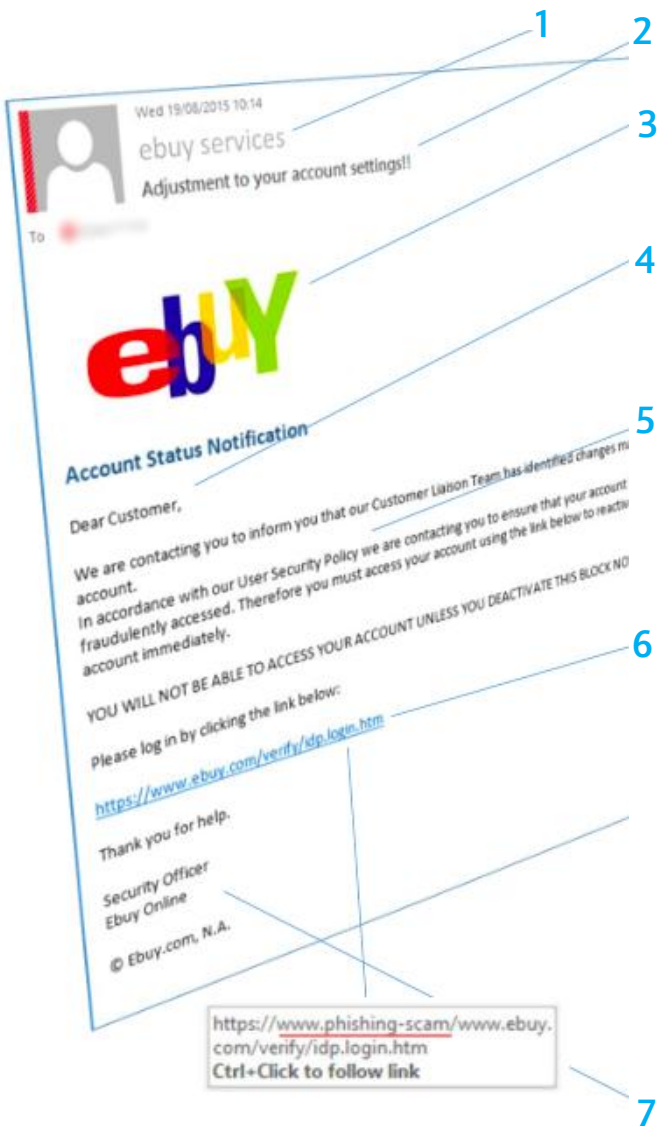
BARCLAYS

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 email – what to look for



1. Sender - Were you expecting this email? Not recognising the sender isn't necessarily cause for concern but look carefully at the sender's name – does it sound legitimate, or is it trying to mimic something you are familiar with?

2. Subject line - Often alarmist, hoping to scare the reader into an action without much thought. May use excessive punctuation.

3. Logo - The logo may be of a low quality if the attacker has simply cut and pasted from a website. Is it even a genuine company?

4. Dear You - Be wary of emails that refer to you by generic names, or in a way you find unusual, such as the first part of your email address. Don't forget though, your actual name may be inferred by your email address.

5. The body - Look out for bad grammar or spelling errors but bear in mind modern phishing looks a lot better than it used to. Many phishing campaigns originate from non-English speaking countries but are written in English in order to target a wider global audience, so word choice may be odd or sound disjointed.

6. The hyperlink/attachment - The whole email is designed to impress on you the importance of clicking this link or attachment right now. Even if the link looks genuine, hover the mouse over it to reveal the true link, as shown in the image below. It may provide a clue that this is not a genuine email. If you are still unsure, do not click the link – just open a webpage and log onto your account via the normal method. If it appears to be from a trusted source, consider phoning the company's customer service, but never follow the email's instructions. Be aware that some companies operate policies stating they will never include links in emails and will never ask for personal information. Again, if in doubt, open a browser and check – and do not open attachments.

7. Signature block - The signature block may be a generic design or a copy from the real company.

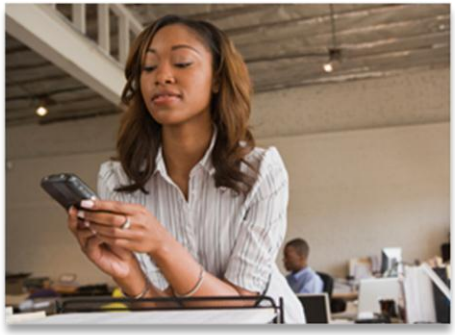
BARCLAYS

Examples of social engineering

Vishing

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 despatch a 'courier' to collect payment cards or other records from you, known as courier fraud.

Smishing



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, 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.

How to avoid Social Engineering attacks

- Never reveal personal or financial data including usernames, passwords, PINs, or ID numbers.
- 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 organisation 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.
- Remember that a bank or other reputable organisation will never ask you for your password or PIN via email or phone call. If you think someone knows your password or PIN change it immediately.

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 – a automated effort to hack your password.
    - Spyware – recording you log in.
    - Shoulder surfing – watching you log in.

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.

Brute Force Attack

Continuously attempting to crack your password. Make sure you have a strong password policy. Use a combination of alpha numeric and special characters. Avoid dictionary words due to password crackers, use 2-factor where possible, don't use common passwords, i.e. Password or 123456, do not store passwords in clear text, different passwords between personal and business. If one password is known and there are similar passwords in other systems, change them.

DDOS Attack

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

Invoice Fraud

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

BARCLAYS

Trojans

- 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:

- Gemalto eSigner never offers automatic updates.
- Never reveal your card number and/or PIN

If this happens:

- remove your Smart Card immediately
- disconnect the infected machine from the network
- contact us for additional support on 0330 1560155. (Calls to 03 numbers use free plan minutes if available. Otherwise they cost the same as 01/02 prefix calls)

You will only ever be prompted to enter you Smart Card and PIN when logging in, authorising a payment or approving an administrative change.

Obeying Orders

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

File | Message

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | More | Awards | Team E-mail | Reply & Delete | To Manager | Done | Create New | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

This message was sent with High importance.

From: Smith, Jon : SB Ltd
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

Every week Barclays has reports of Cyber Fraud from people, organisations and businesses where a successful 'con' trick has worked, and the criminal has fooled somebody into doing something they shouldn't…

BARCLAYS

Fraud smart tips – Cheques – receiving

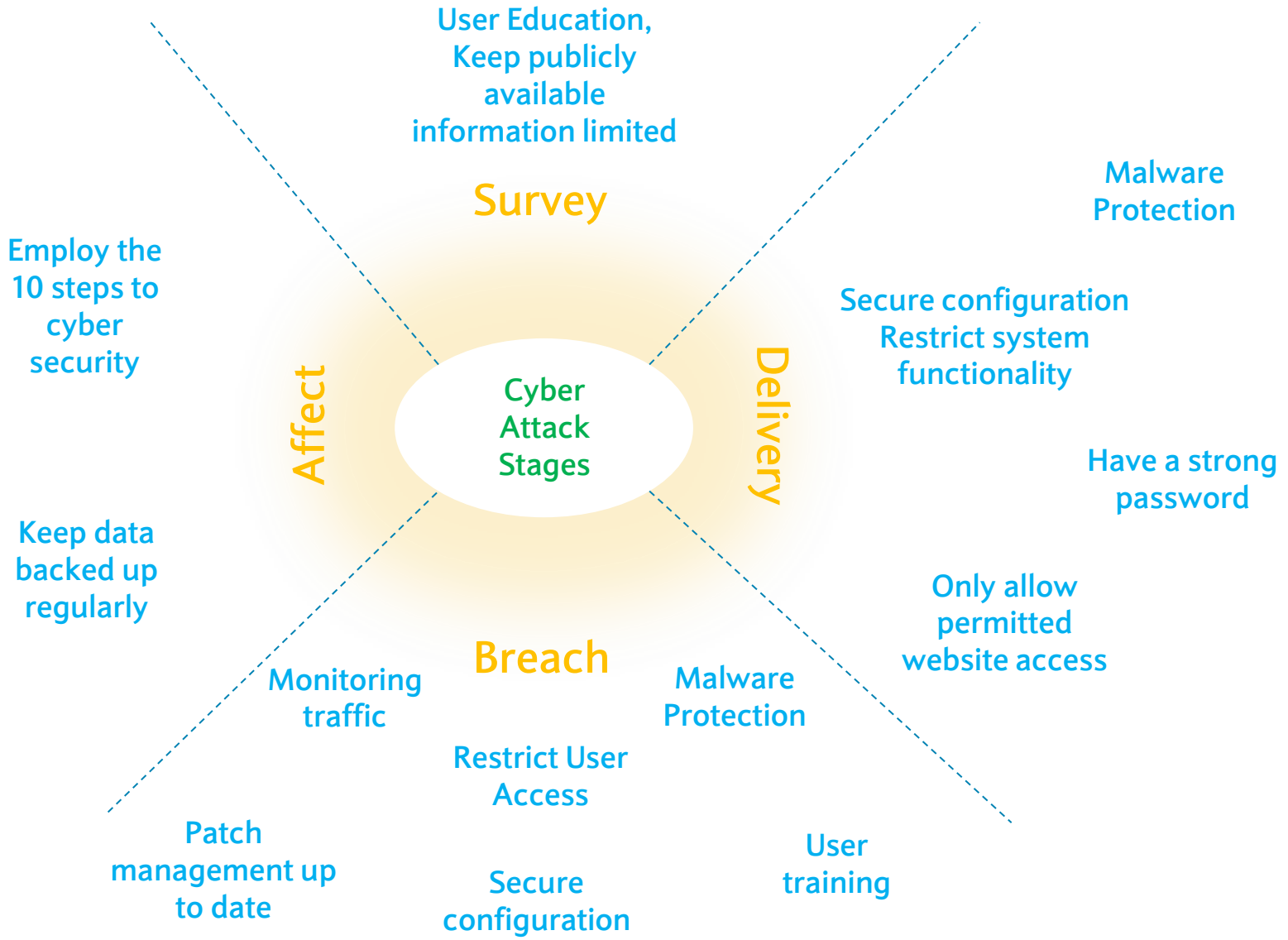
- Be alert to unexplained or unexpected credits to your account
- Be sure the funds are cleared before you deliver goods or provide services
- Don't be fooled by the narrative it does not mean the funds are cleared
- Never pay any refunds to somebody against **uncleared** funds
- If in doubt speak to 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

Reducing the impact of cyber attacks – The 4 stages

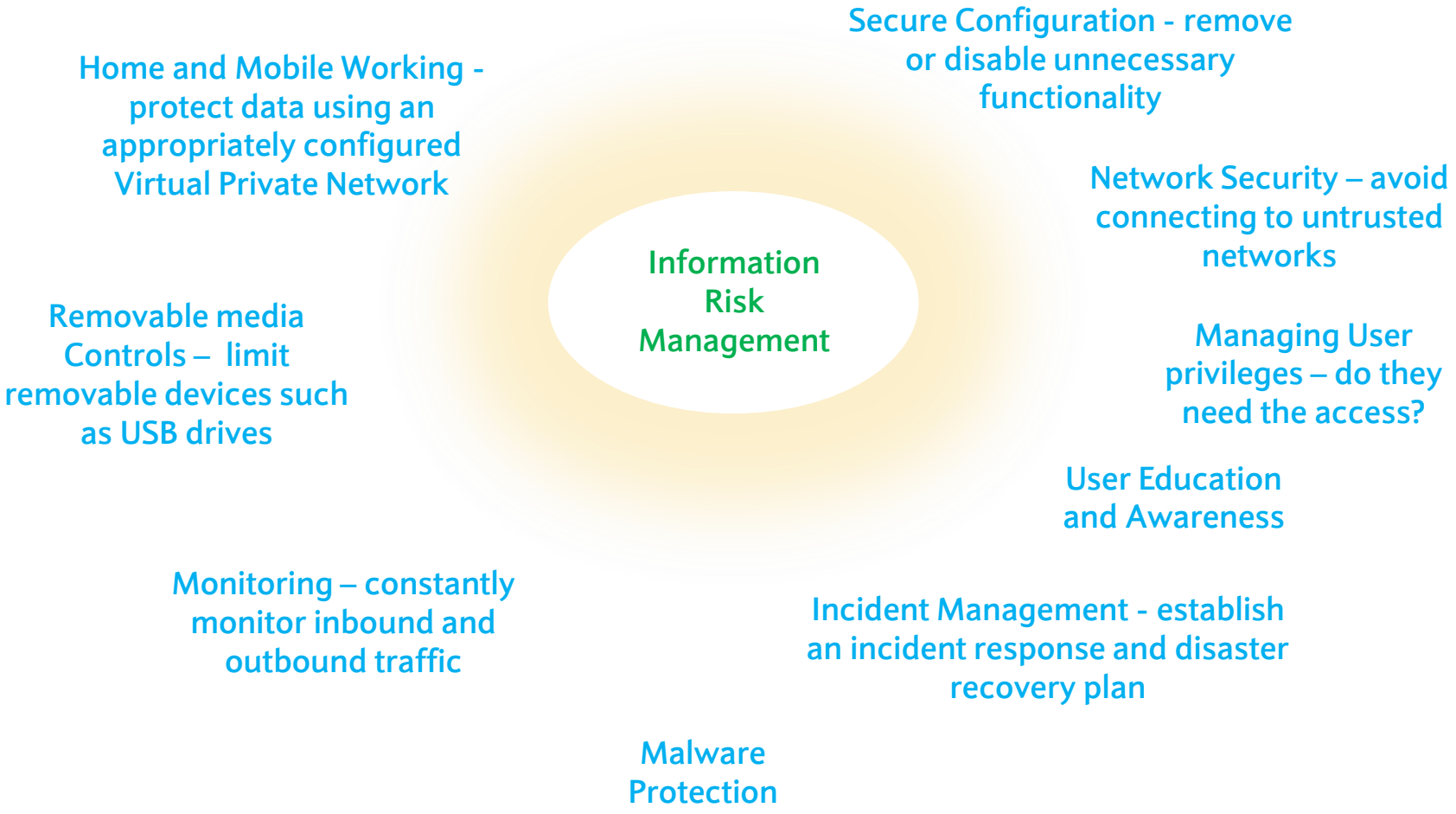


Credit CESG

BARCLAYS

10 steps to cyber security – some basic guidance

"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

BARCLAYS

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

CERT-UK is the national computer response team and work towards enhancing the UK's cyber resilience

CiSP
A CATALYST FOR COLLABORATION

CERT-UK 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.

Barclays Services Are Secure – The Barclays Promise

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.

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.

Further reading

- www.digitaldrivinglicence.barclays.co.uk - 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.cyberstreetwise.com - HM Government site – Be Cyber Streetwise is a cross-government campaign funded by the National Cyber Security Programme
- www.cyberstreetwise.com/cyberessentials - Cyber Essentials – new Government-backed and industry supported scheme to guide businesses in protecting themselves against cyber threats
- www.cert.gov.uk - Working with partners across industry, government and academia to enhance the UK's cyber resilience
- www.actionfraud.police.uk - The UK's national fraud and internet crime reporting centre
- www.barclayscorporate.com/information/fraud-videos.html - A list of videos explaining the types of social engineering fraud used by cyber criminals
- https://www.getsafeonline.org/ - An online resource of advice about staying safe while online

BARCLAYS

Any questions?

BARCLAYS