adapta

Data protection, information security and cake

7 February 2024

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE

CFG INSPIRING FINANCIAL LEADERSHIP

Crown Commercial Service Supplier

We are a Living Wage Employer

About Adapta

- We are a **specialist** information systems consultancy
- We only work with **charities**, associations, trusts and others in the not-for-profit sector
- We are completely **supplier-independent**
- Our consultants have held **senior** positions in a broad range of different organisations
- Our advice and guidance is based on **practical experience** gained over many years

About Adapta

- Digital, Data & Technology Strategies
- Reviews & Health Checks
- Business Processes & System Requirements
- Supplier & Solution Selection
- Interim Technical Leadership
- Programme & Change Success
- Risk, Compliance, Data Protection & Security
- Governance & Business Cases
- Digital Workforce & Operating Models

FIRE
BREAK GLASS
PRESS HERE

Some of the areas we'll be looking at today

- Overview of common risks and potential pitfalls
- What good practice looks like
- Effective strategies and practical tips to ensure that you're well-prepared
- An update on relevant standards and legislation
- Some learnings from 'real life'
- An opportunity to ask questions and discuss your own issues

Programme

14:00	**Arrival and welcome** Welcome - introductions and overview of the agenda for the afternoon.
14:10	**Information security – what's new in the sector?** Paul Sypko, Adapta Consulting
14:30	**Data Protection update** Carla Whalen, Russell-Cooke
15.00	**Mid-afternoon break (tea/coffee and more cake)**
15.15	**Case study** Cheryl Hodgson, Motability Foundation
15:45	**Roundtable discussion & feedback** All
16.30 - 17.00	**Review & close** Paul Sypko, Adapta Consulting

Introductions

Information security – what's new in the sector?

Paul Sypko, Partner, Adapta

Exhibit 1: A typical Data Protection conference

Exhibit 2: Information Security not so long ago

An existential threat? Cyber security incidents can have an impact far beyond the data protection consequences alone

- Disruption to operations, ability to serve the cause
- Impact on data subjects
- Financial cost and losses – ransoms, fraud and fines
- Reputation

Different but complementary perspectives

Important but technical and a bit complicated?
→ ***Good practice but left to our discretion?***

"The EU"… "Acts of Parliament"… "The Law"… "Regulations"… "Safeguarding and protection"
→ ***No choice. A legal necessity?***

NFPs *do* matter… security isn't just for banks etc

Charities in England & Wales spend **£80Bn** per year

58% of charities think cybercrime is a major risk to the charity sector

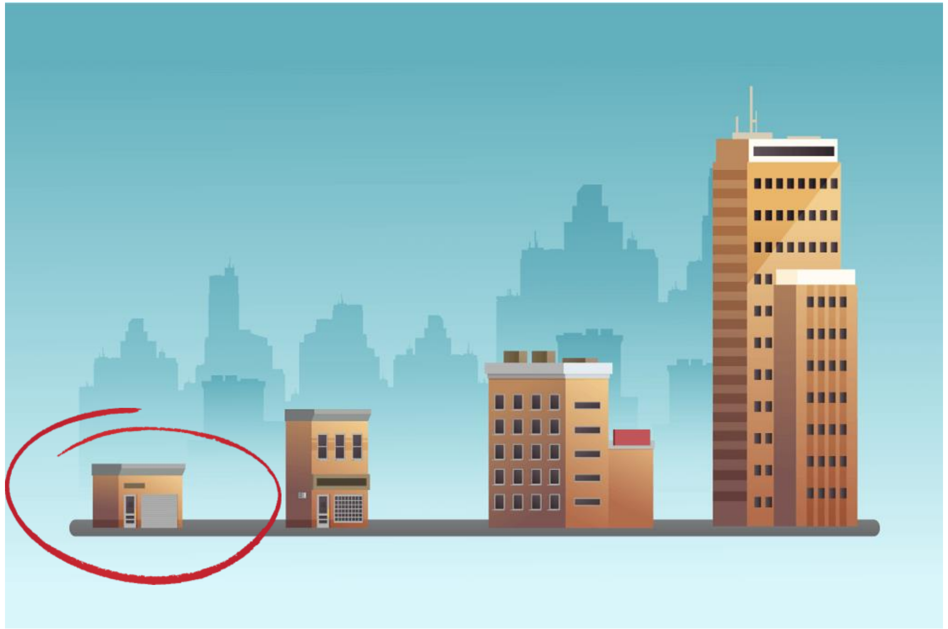
22% believe cybercrime is a greater risk to the charity sector than other sectors

<u>Source</u>: Preventing Charity Cybercrime: Insights+Action. Charity Commission Fraud Advisory Panel. Sample of 15,000 charities.

…and cybercrime is now a very likely cause of a major security or data breach in an NFP

- Money (even the small ones)
- Reputations worth protecting
- Lots of valuable intellectual property…

+



Not many staff – maybe their procedures and IT security aren't as strong as 'tougher targets'?

Principle 6 of UK GDPR

Article 5(1) of the UK GDPR requires that personal data shall be:

“…processed in a manner that ensures appropriate security of the personal data, including **protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** (‘integrity and confidentiality’).”

‘Data protection by default’ – often overlooked?

Article 25(2) of UK GDPR:

“The controller shall implement appropriate technical and organisational measures for ensuring that, **by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.”

What do people usually think are the main risks?

- **Phishing** – ‘Dear accounts team, Pay this invoice immediately. Yours sincerely, the CEO’ (54%)
- **Ransomware** – ‘Send us some bitcoins if you want your files unencrypted’ (31% including extortion)
- **Extortion** – ‘Give us some money or we’ll leak your data on the dark web’
- **DDoS** – ‘Botnet’ attacks to overwhelm and take an organisation’s systems ‘down’ (5%)
- **Social engineering** – Pretending to be someone else (e.g. you!), diverting donations

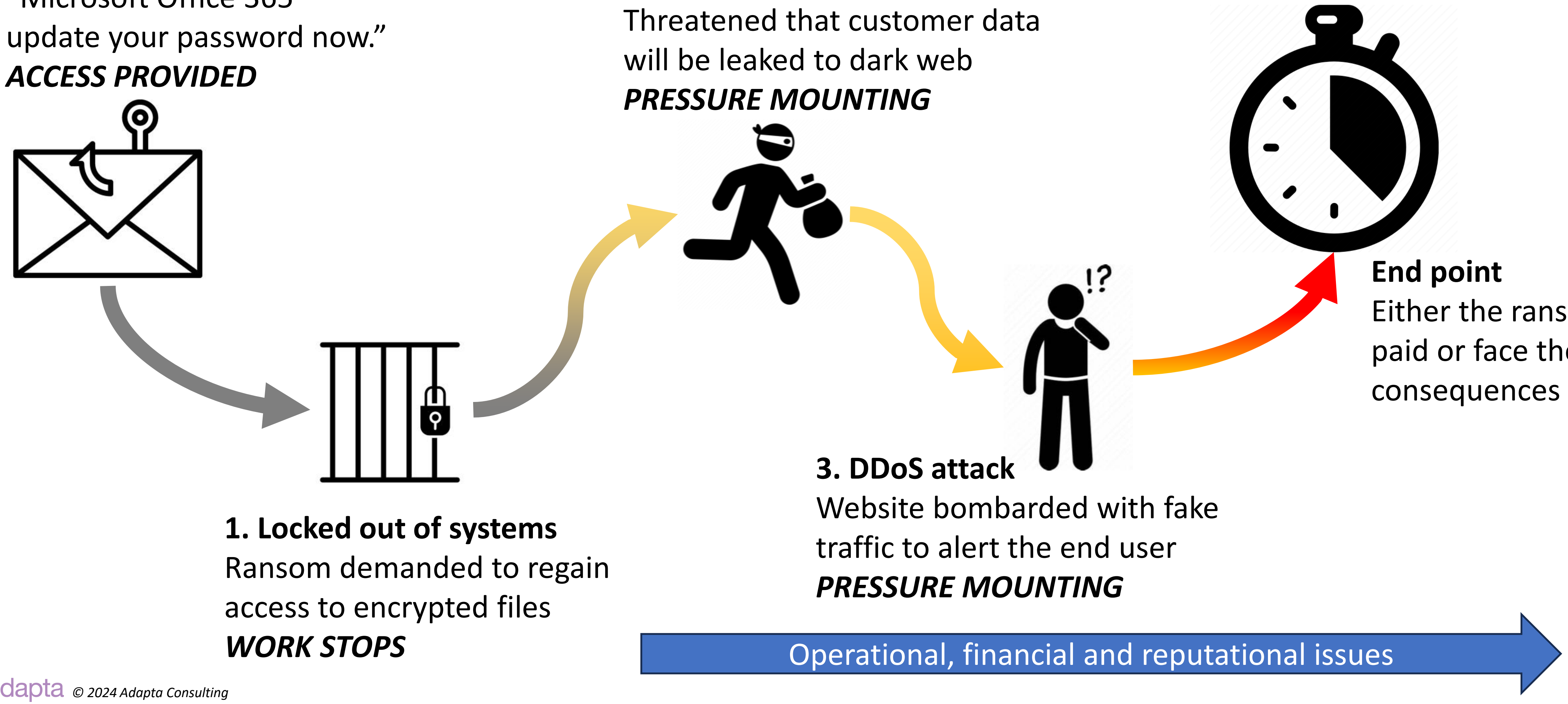
Can you think of any others?

Can you think of any others?

- AI - Deepfake scams, highly targeted phishing
- Impersonation (e.g. to customers, suppliers)
- Human error!

WEF Study: 95% of cyber security incidents occur due to human error

A potential real-life scenario – triple extortion



Phishing campaign
“Microsoft Office 365 – update your password now.”
ACCESS PROVIDED

1. Locked out of systems
Ransom demanded to regain access to encrypted files
WORK STOPS

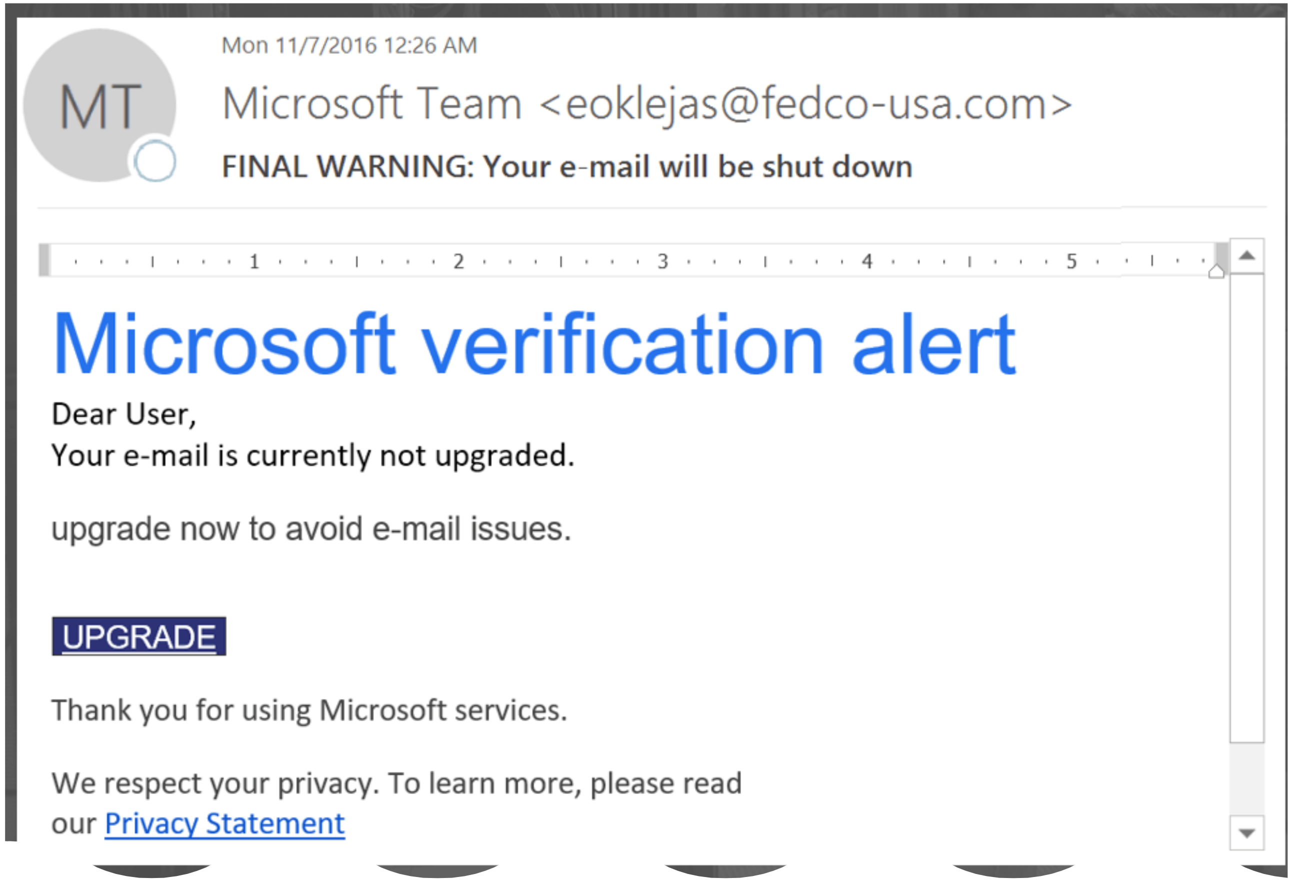
2. Data exfiltrated
Threatened that customer data will be leaked to dark web
PRESSURE MOUNTING

3. DDoS attack
Website bombarded with fake traffic to alert the end user
PRESSURE MOUNTING

End point
Either the ransom is paid or face the consequences

Operational, financial and reputational issues

Attacks are getting smarter… AI is helping with this



Mon 11/7/2016 12:26 AM

Microsoft Team <eoklejas@fedco-usa.com>

FINAL WARNING: Your e-mail will be shut down

Microsoft verification alert

Dear User,
Your e-mail is currently not upgraded.

upgrade now to avoid e-mail issues.

UPGRADE

Thank you for using Microsoft services.

We respect your privacy. To learn more, please read our Privacy Statement

Spot the difference…

www.lloydsbank.co.uk

is not the same as

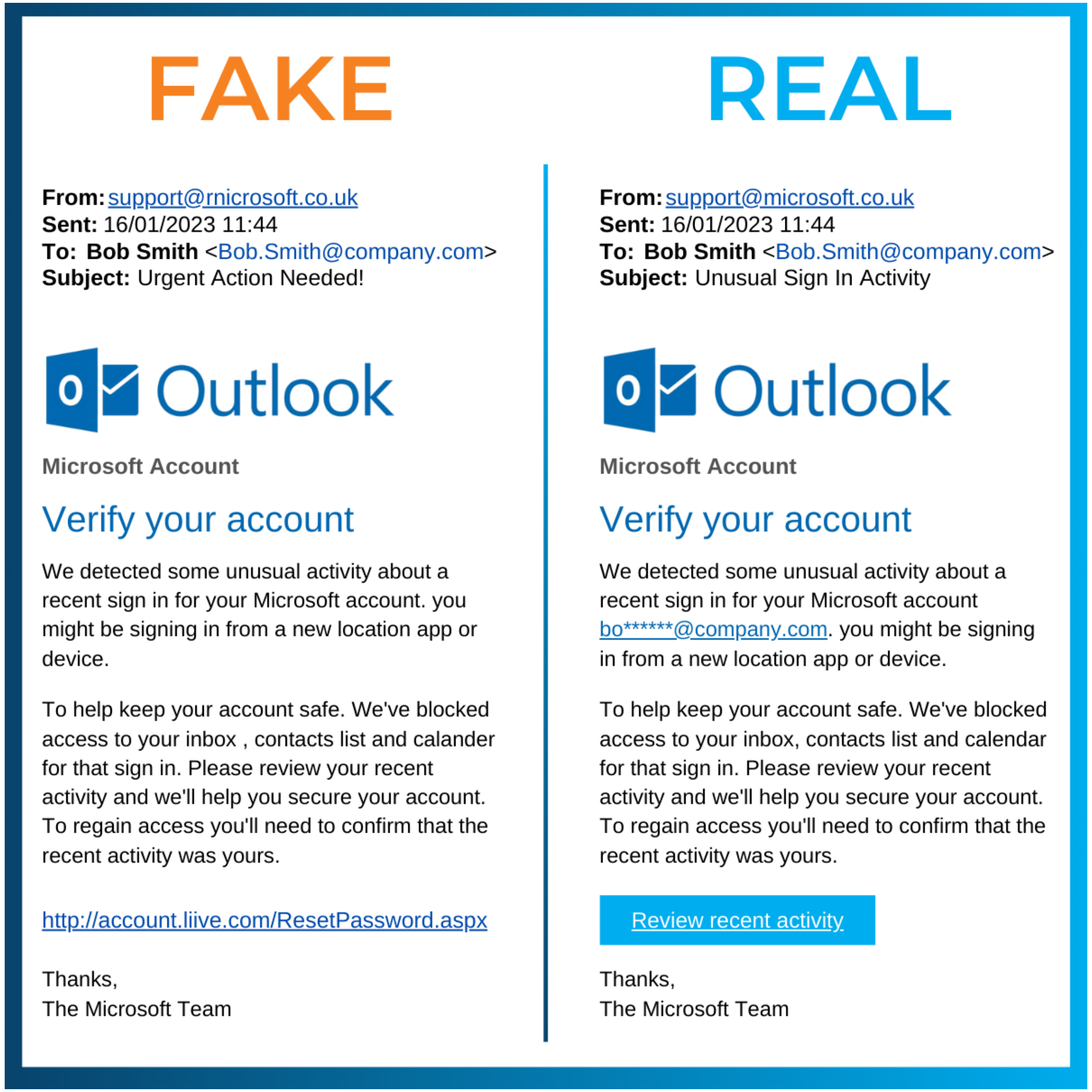
www.lloydsbank.co.uk

www.natwest.co.uk

is not the same as

www.natwest.co.uk

Educating staff and raising awareness…



FAKE

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

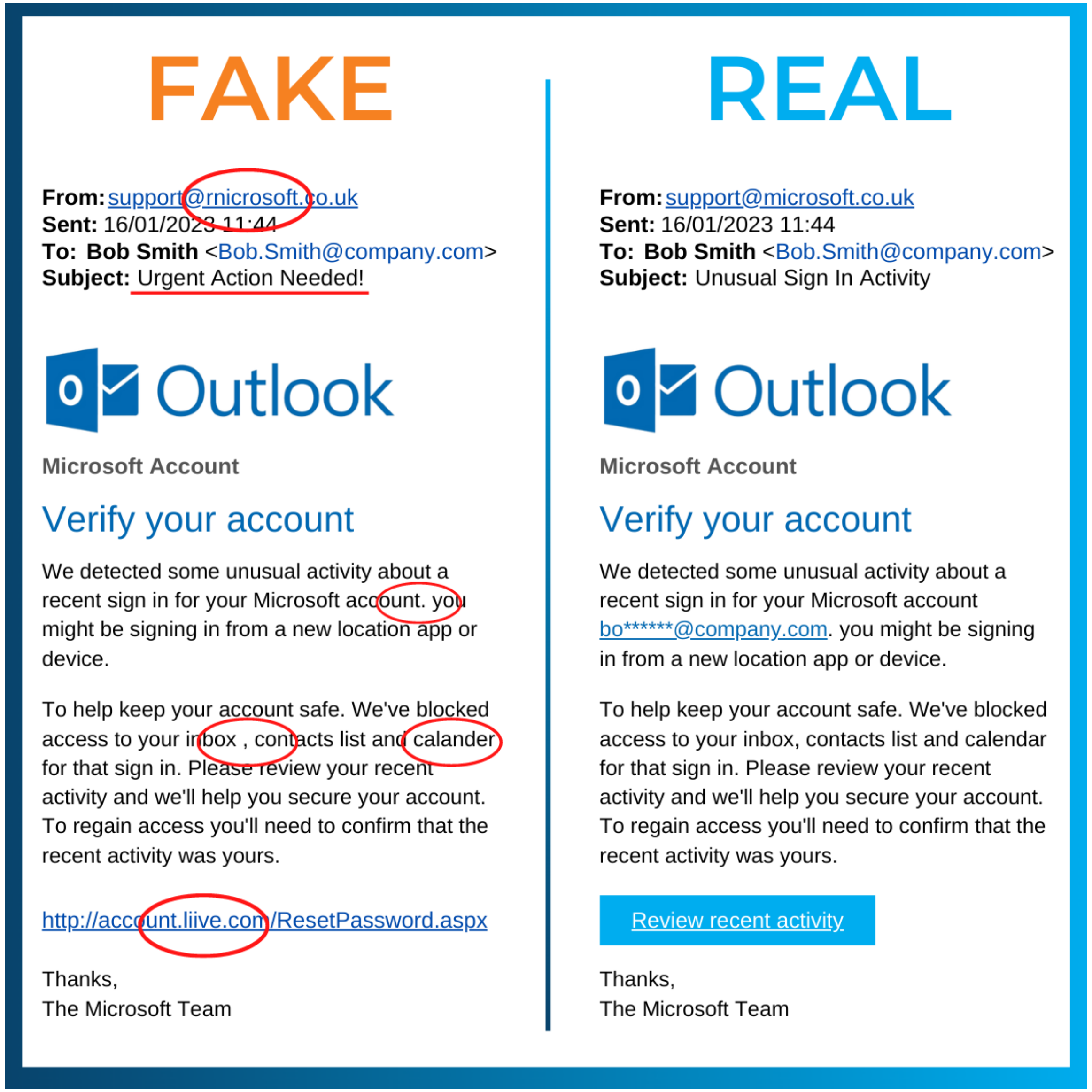
To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Thanks,
The Microsoft Team

Spot the difference

(6 differences to find)

Educating colleagues…



FAKE

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

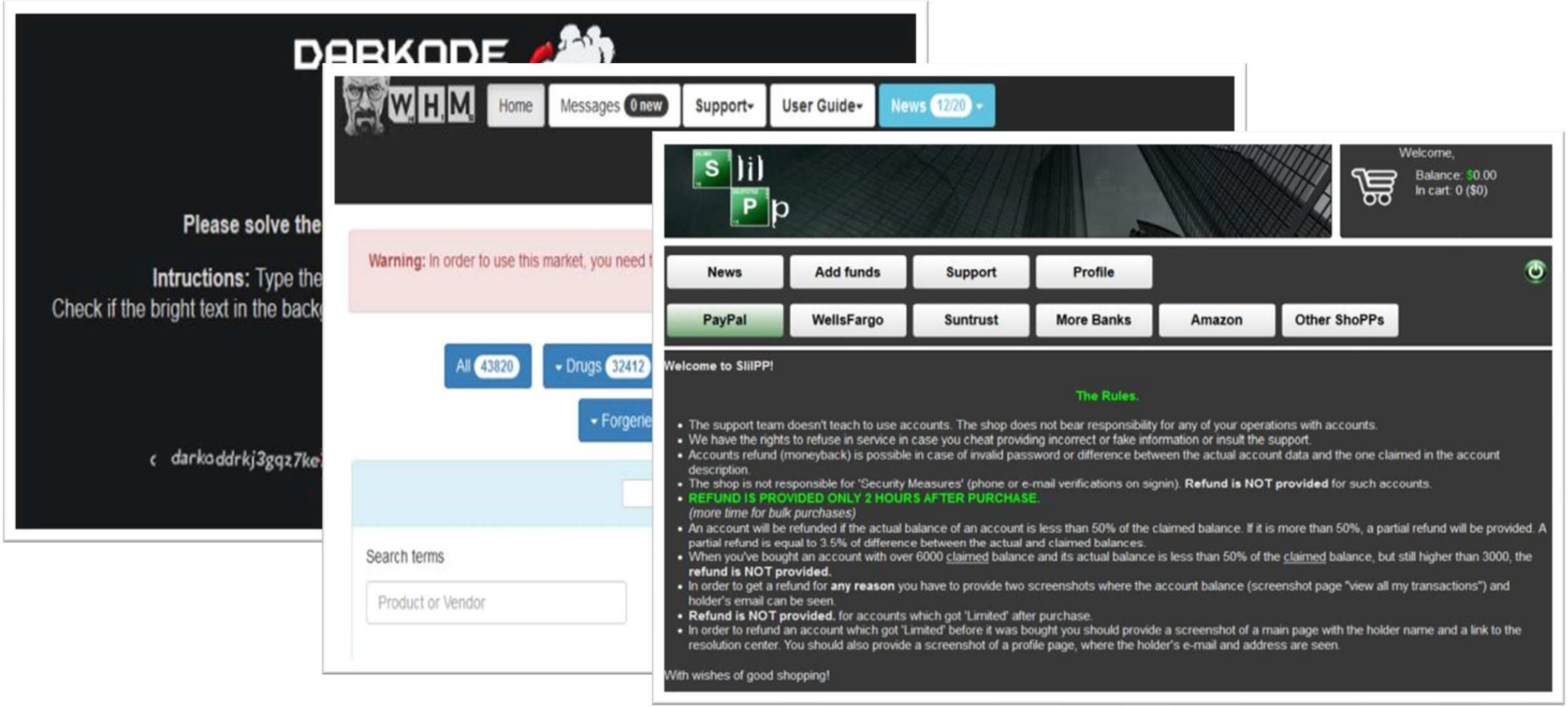
We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

A boom in phishing: ‘Cyber-crime as a Service’



Please solve the

Intructions: Type the
Check if the bright text in the back

darkoddrkj3gqz7ke

Warning: In order to use this market, you need t

Welcome to SiiPP!

The Rules.

- The support team doesn't teach to use accounts. The shop does not bear responsibility for any of your operations with accounts.
- We have the rights to refuse in service in case you cheat providing incorrect or fake information or insult the support.
- Accounts refund (moneyback) is possible in case of invalid password or difference between the actual account data and the one claimed in the account description.
- The shop is not responsible for 'Security Measures' (phone or e-mail verifications on signin). **Refund is NOT provided** for such accounts.
- **REFUND IS PROVIDED ONLY 2 HOURS AFTER PURCHASE.**
  (more time for bulk purchases)
- An account will be refunded if the actual balance of an account is less than 50% of the claimed balance. If it is more than 50%, a partial refund will be provided. A partial refund is equal to 3.5% of difference between the actual and claimed balances.
- When you've bought an account with over 6000 claimed balance and its actual balance is less than 50% of the claimed balance, but still higher than 3000, the **refund is NOT provided.**
- In order to get a refund for **any reason** you have to provide two screenshots where the account balance (screenshot page "view all my transactions") and holder's email can be seen.
- **Refund is NOT provided.** for accounts which got 'Limited' after purchase.
- In order to refund an account which got 'Limited' before it was bought you should provide a screenshot of a main page with the holder name and a link to the resolution center. You should also provide a screenshot of a profile page, where the holder's e-mail and address are seen.

With wishes of good shopping!

Everyone likes an easy fix!

Pen testing!

The Cloud!

More tech!

SecOps!

ISO27001!

A better place to start?

WATCH THIS HACKER BREAK INTO MY CELL PHONE ACCOUNT IN 2 MINUTES

What to think about in your plans…

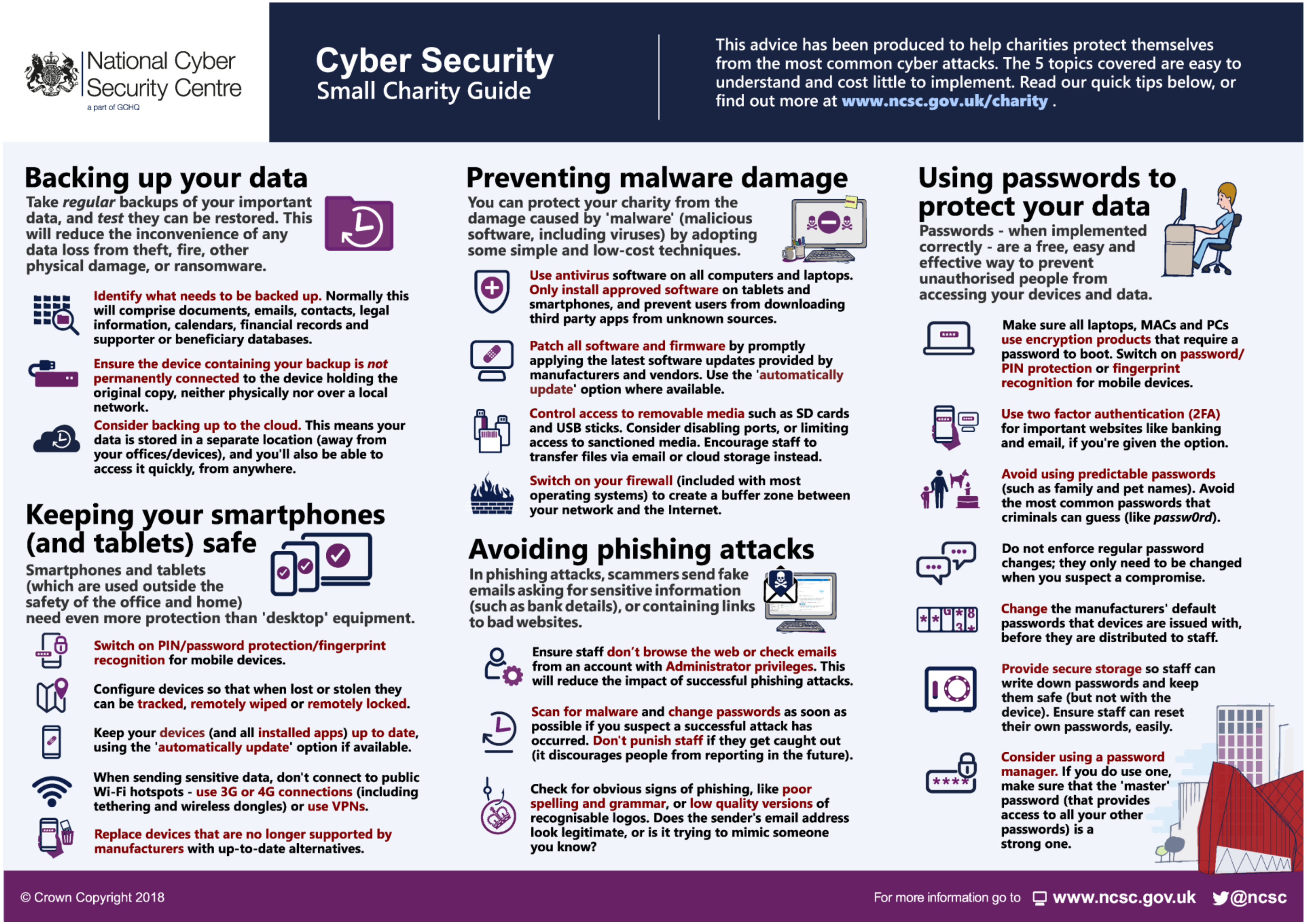
- Governance and 'organisational measures' – **clarifying responsibilities**
- Your **procedures and checks** for making payments
- **Backups and immutability**
- Resourcing and capabilities
- **Supply chain vulnerabilities**
- **MFA and 'account hygiene'**
- Endpoint management
- Staying current

- Choosing appropriate standards to adopt
- Auditing suppliers and doing due diligence
- **Security culture** / getting people involved
- Patching and network management
- **Training and awareness**
- Pen testing
- Data Protection & Digital Information Bill
- Cyber insurance
- Incident response plans – thinking ahead
- Volunteers, trustees – data outside the organisation

Standards and regulations

- Data Protection Act 2018 incorporating the UK GDPR

- Compliance is an ongoing/continuous process, not a one-off exercise
- Standards are a good place to start (Cyber Essentials, ISO 27001)
- Regular external reviews and advice
- Lean on trusted partners – pragmatic ones!
- Events, conferences – like this one!
- News and publications (the register, etc)
- NCSC website



National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

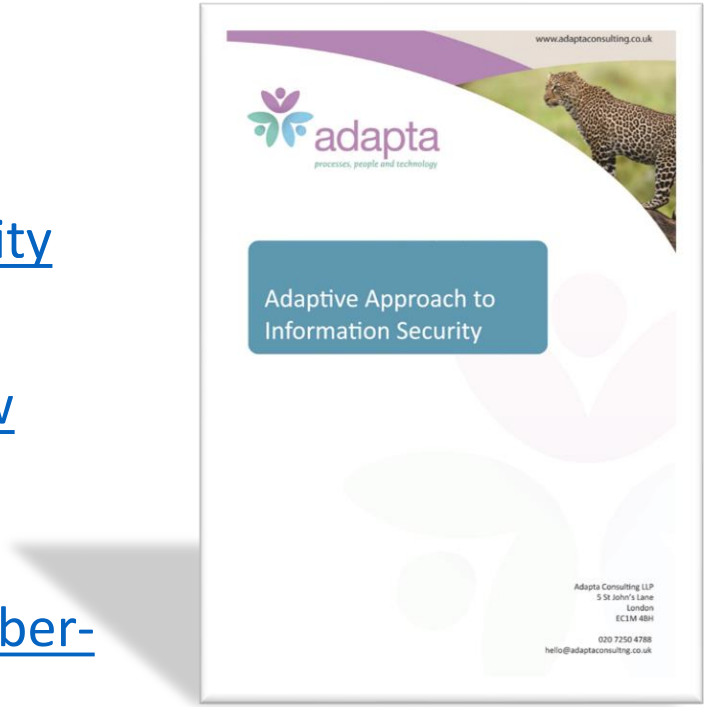
Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

Gaining support by 'making it real' on a personal level

Other useful resources

- National Cyber Security Centre (NCSC) – 10 steps to cyber security https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
- NCSC Small Charity Guide - https://www.ncsc.gov.uk/collection/charity
- Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview
- Preventing Charity Cyber Crime (Charity Commission) - https://www.gov.uk/government/publications/preventing-charity-cyber-crime-insights-and-action
- Charity Security Forum - https://charitiessecurityforum.org.uk/



www.adaptaconsulting.co.uk

adapta
processes, people and technology

Adaptive Approach to
Information Security

Adapta Consulting LLP
5 St John's Lane
London
EC1M 4BH

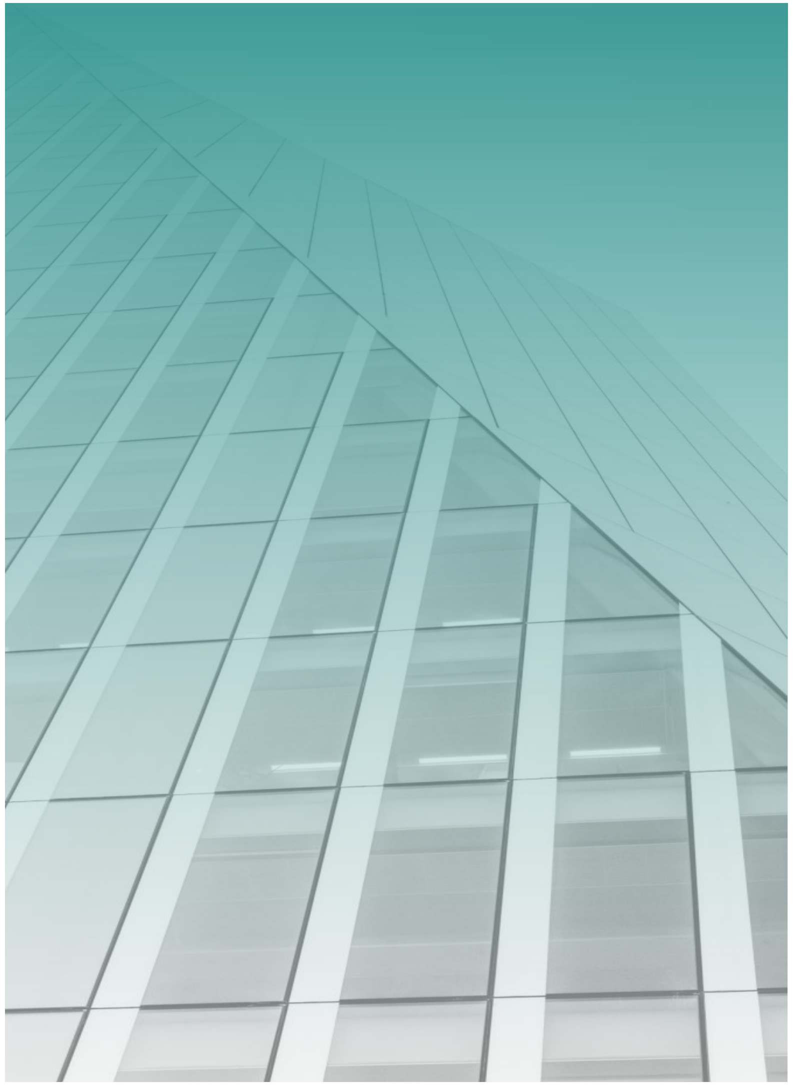
020 7250 4788
hello@adaptaconsultng.co.uk

Data Protection update

Carla Whalen, Partner, Russell-Cooke

DATA PROTECTION UPDATE

CARLA WHALEN, PARTNER



What’s new? - DPDI Bill

- A truly bespoke, British system of data protection?
- Currently making its way through House of Lords – return to Commons for final consideration
- Expected this year – general election could disrupt

Charities and the soft opt-in

- Will be able to use the soft opt-in for direct marketing that's **solely for the purpose of furthering a charitable or other non-commercial objective** – no need for consent!
- **As long as:**
    - the contact details were obtained in the course of the recipient expressing an interest in, or offering or providing support for, the furtherance of that objective or a similar objective – i.e. **existing** supporters, donors etc.
    - the recipient has been given a simple **means of opting-out** at the time their details were collected and in each subsequent email

Legitimate interests (LI)

- LI purposes can include processing:
  - that’s necessary for the purposes of **direct marketing**
  - for **intra-group data transfers** (e.g. employees, supporters, service users) where necessary for internal administrative purposes
  - that’s necessary to ensure the **security of network and information systems**
- List of **recognised LIs** – no need for the balancing test

Recognised LIs include:

- **Emergencies**
- **Crime**
- **Safeguarding**

Reducing the compliance burden

- DPOs to be replaced by **senior responsible individuals**
- **Duty to keep records** limited to processing likely to result in a high risk to the rights and freedoms of individuals
- **New threshold for refusing or charging** people to comply with requests to exercise individual rights – “vexatious or excessive”
- **Changes to cookie consents** – no need for consent to use of non-intrusive cookies (e.g. analytics)

Recent ICO guidance

- **Guidance:** dealing with SARs in employment https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/subject-access-request-q-and-as-for-employers/
- **Guidance:** sending bulk communications by email: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/email-and-security/
- **Guidance:** 10-steps – sharing information to safeguard children: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/

ICO updates and consultations

- **Consultation:** employment and data protection – keeping employment records; recruitment and selection
- **Updates:** employment and data protection – using HR health information; monitoring workers

  https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/
- **Opinion:** Children's code – clarification on how to comply with age assurance https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/01/ico-publishes-updated-commissioner-s-opinion-on-age-assurance-for-the-children-s-code/

Carla Whalen

☎ 020 8394 6419

✉ Carla.Whalen@russell-cooke.co.uk

Carla combines expertise in employment law and data protection with experience and understanding of the not-for-profit sector.

She is able to call on her HR, regulatory and safeguarding knowledge to get to the bottom of knotty problems and offer creative solutions.

Russell-cooke.co.uk

This material does not give a full statement of the law. It is intended for guidance only and is not a substitute for professional advice. No responsibility for loss occasioned as a result of any person acting or refraining from acting can be accepted by Russell-Cooke LLP.

Russell
Cooke

Break

Client case study

Cheryl Hodgson, Risk Controls and Compliance Manager, Motability Foundation

Motability Foundation

Data Protection Journey

07 February 2024

Motability Foundation

Contents

1. Introduction
2. Who are Motability Foundation?
3. What do we do?
4. How did we introduce GDPR?
5. What challenges did we encounter?
6. What challenges do we still encounter?
7. What worked for us?
8. What next?

Motability Foundation

Introduction

Cheryl Hodgson
Data Protection Officer
Motability Foundation

Motability Foundation

Who are Motability Foundation?

Our Vision:

We are building a future where all disabled people have the transport options to make the journeys they choose.

Motability Foundation

What do the Motability Foundation do?

We fund, support, research and innovate to help all disabled people make the journeys they choose.

- Oversee the Motability Scheme;
- Provide grants to help people use the Scheme;
- Provide access to transport;
- Award grants to other charities towards making transport accessible;
- Carry out ongoing research;
- Inspire innovations to champion accessible transport.

Motability Foundation

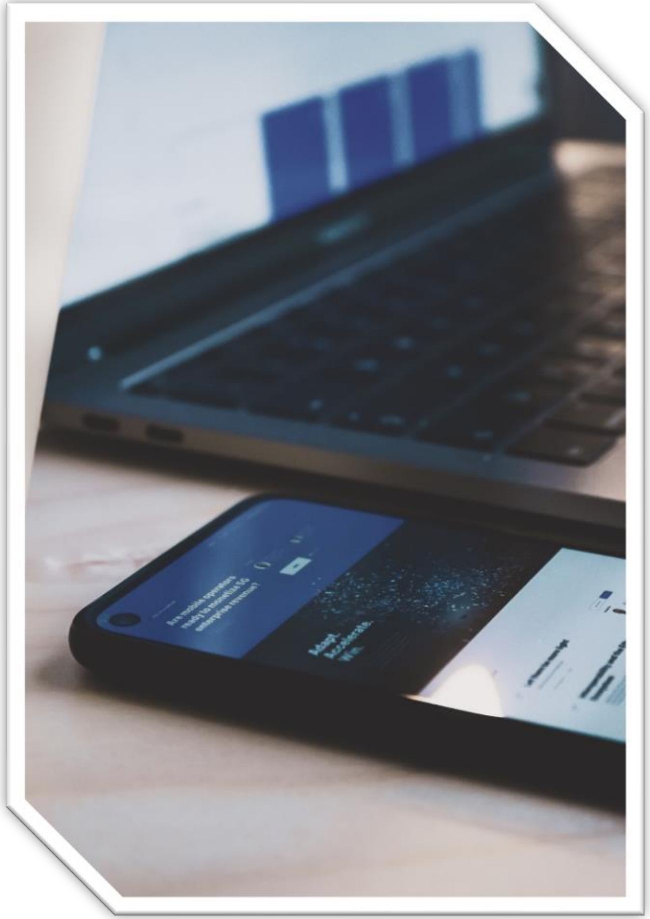
Types of data we process

Personal Data

Special Category Data

- Name and nature of disability;
- Details of the impact this has on mobility;
- Photographs or Videos;
- Third Party data;
- Childrens’ data.

Data Relating to Criminal Convictions

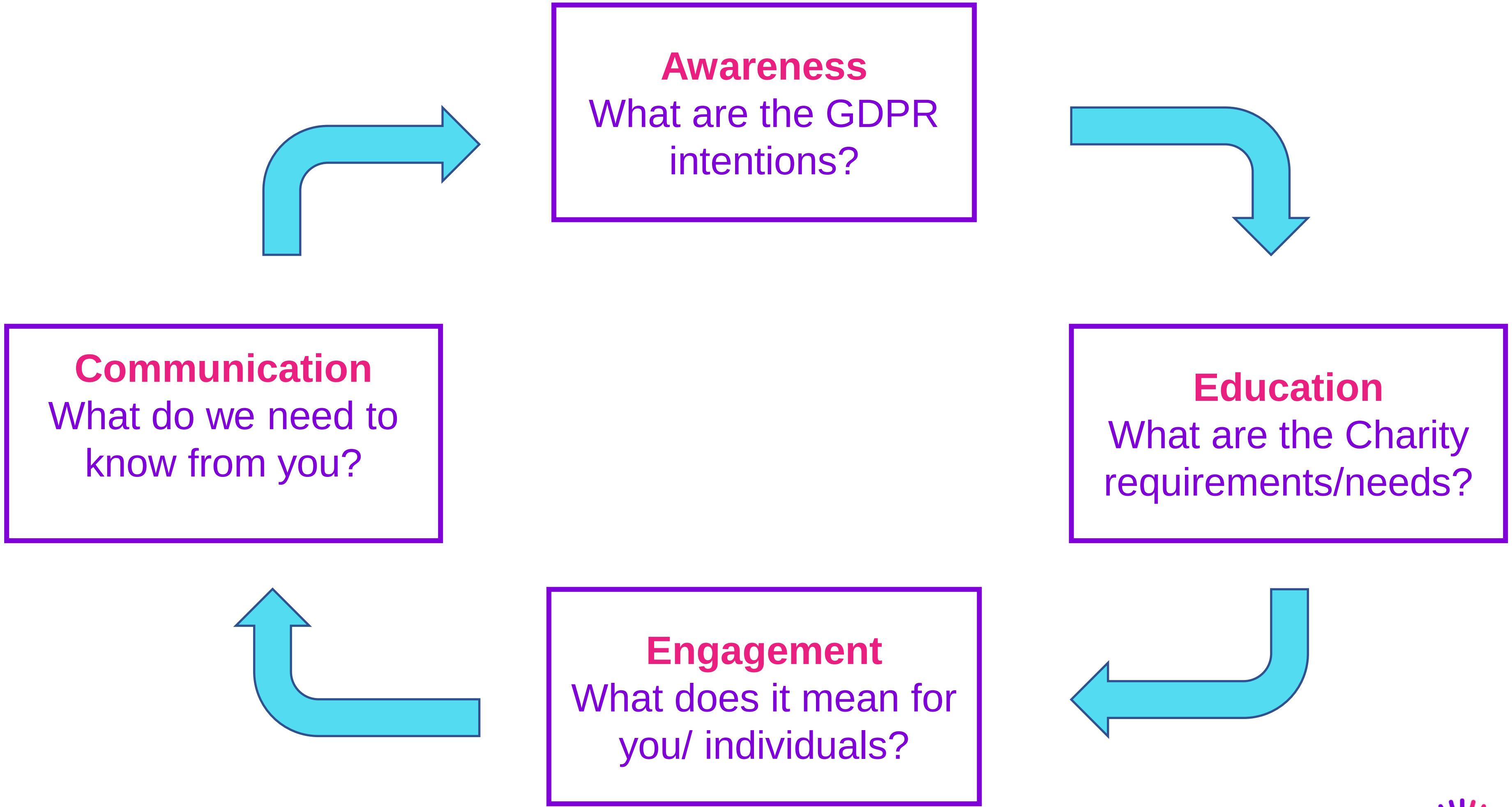


Motability Foundation

How did Motability Foundation Implement their GDPR Strategy?

Motability Foundation

Implementation of GDPR Strategy



Awareness
What are the GDPR intentions?

Education
What are the Charity requirements/needs?

Engagement
What does it mean for you/ individuals?

Communication
What do we need to know from you?

Motability Foundation

What challenges did we encounter?

Motability Foundation

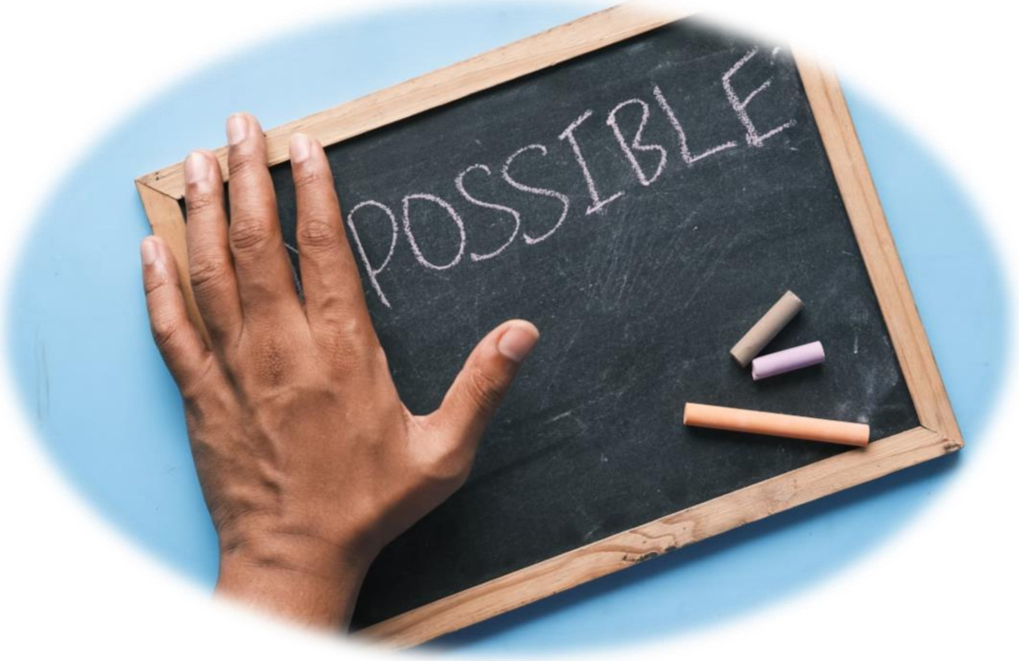
Challenges Encountered

Accountability - Getting people on board;

Getting management support.

The timeframe.

Project Involvement.



Motability Foundation

What challenges do we still face?

What processes do we have to overcome them?

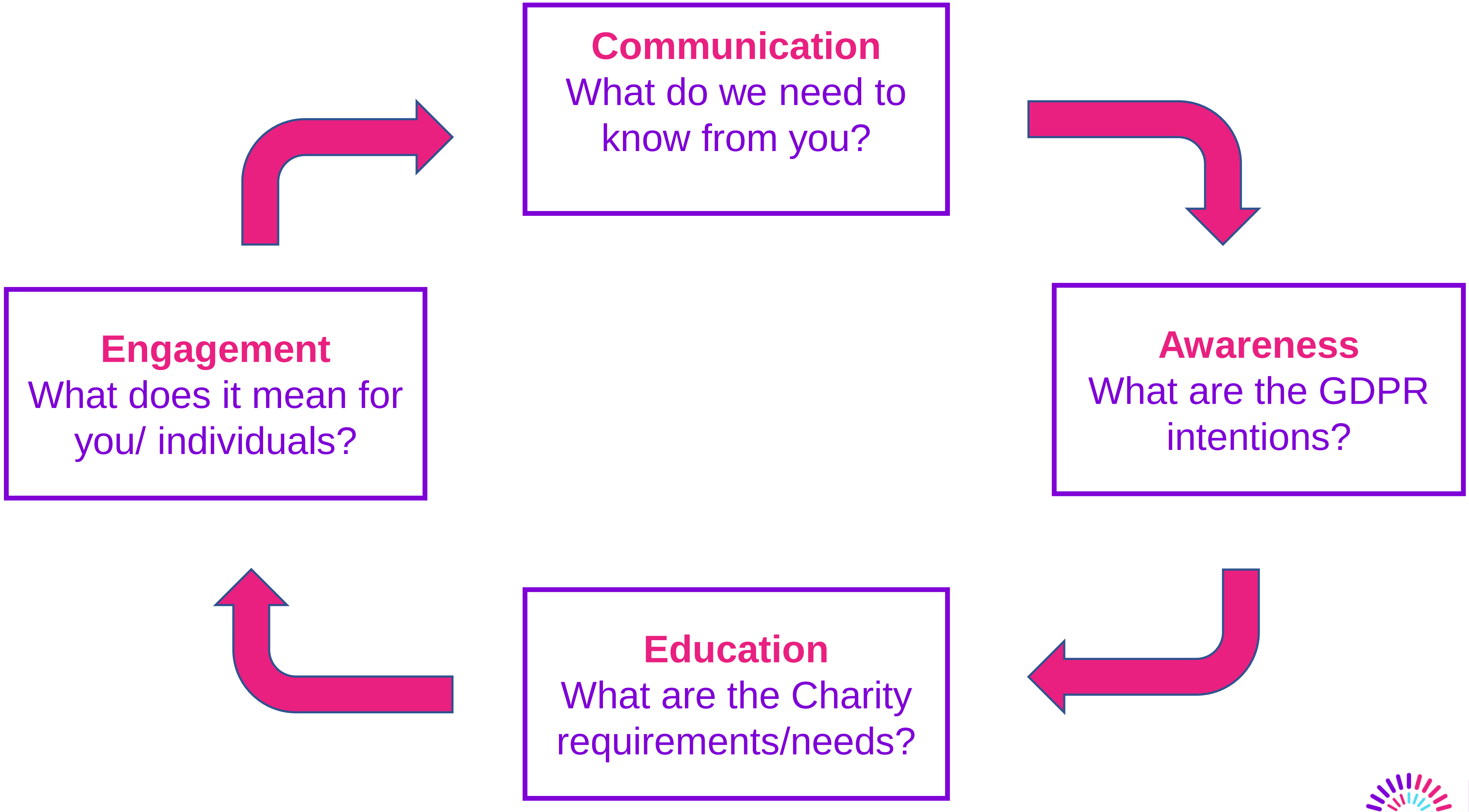
Motability Foundation

Processes to overcome Challenges

- Ask for feedback;
- Awareness-Raising;
- Education;
- Repetition.

Motability Foundation

Implementation of GDPR Strategy



Communication
What do we need to know from you?

Awareness
What are the GDPR intentions?

Education
What are the Charity requirements/needs?

Engagement
What does it mean for you/ individuals?

Motability Foundation

So, what has worked for us?

Motability Foundation

What has worked?

- **Undertaking new starter inductions;**
- **Encourage people to share breaches and near misses;**
- **DPIA Process;**
- **GDPR Champions** – cross departmental meetings;
- **Working with business partners;**
- **DSAR Process.**

Motability Foundation

What next?

- **Relevant training** – used examples from the Motability Foundation;
- **Workshops to support teams with Data Protection;**
- **DP Team training and development;**
- **Email retention;**
- **Communication.**

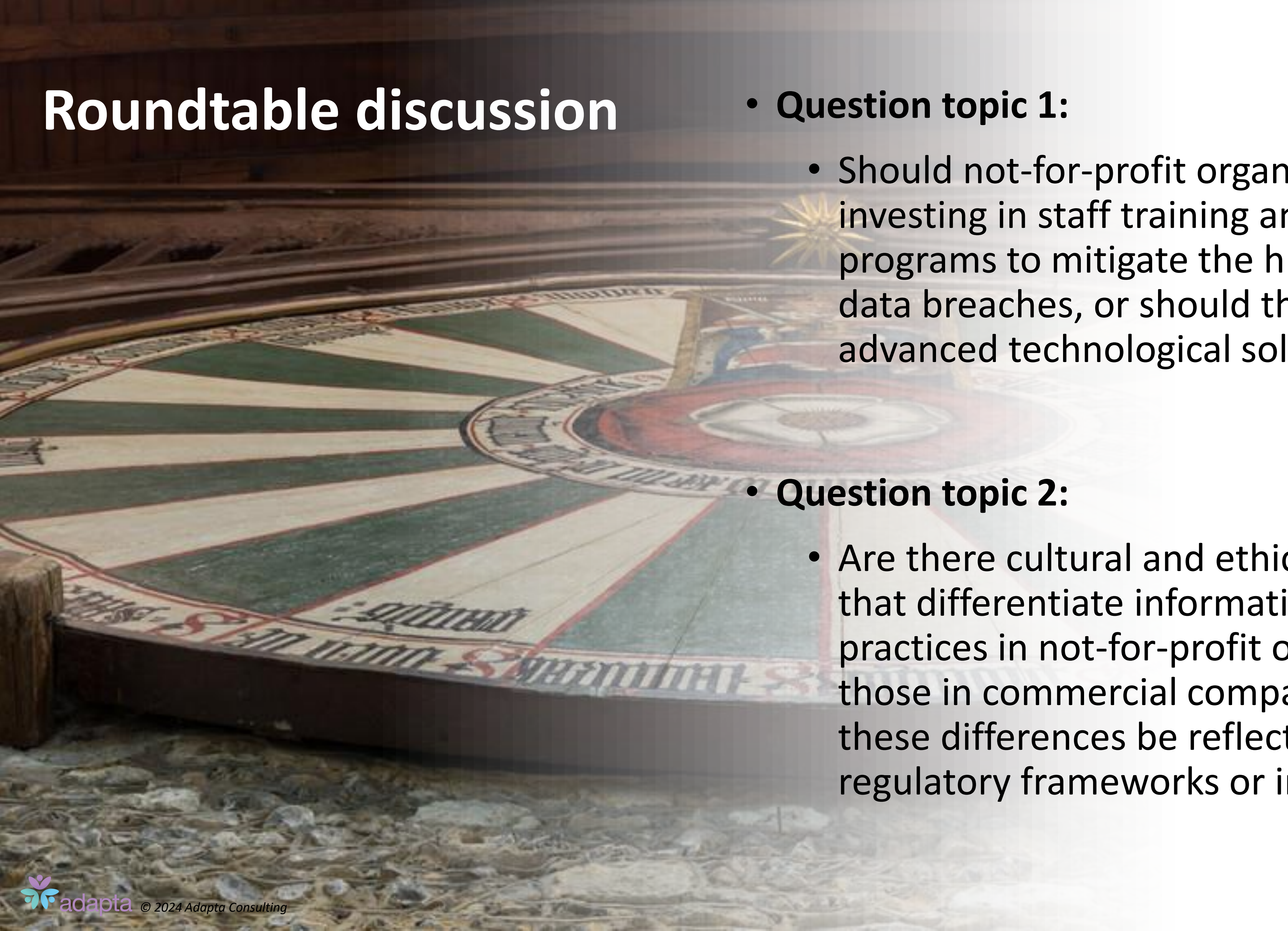
Motability Foundation

Thank you

Cheryl Hodgson
Data Protection Officer

Cheryl.Hodgson@motabililtyfoundation.org.uk

Motability Foundation



Roundtable discussion

- **Question topic 1:**
  - Should not-for-profit organisations prioritise investing in staff training and awareness programs to mitigate the human factor in data breaches, or should they focus more on advanced technological solutions?
- **Question topic 2:**
  - Are there cultural and ethical considerations that differentiate information security practices in not-for-profit organisations from those in commercial companies, and should these differences be reflected in tailored regulatory frameworks or industry standards?

Event feedback

Please use the QR code to view and complete the online feedback form.

Thanks & Goodbye!

adapta

processes, people and technology

Upcoming events…

AI – What it means for charities

6 March 2024, 2pm-3.15pm

Virtual Zoom event.

www.adaptaconsulting.co.uk/adapta-events

hello@adaptaconsulting.co.uk

www.adaptaconsulting.co.uk

5 St John’s Lane, London, EC1M 4BH

☎ 020 4558 8070

We hope you find this presentation enjoyable and thought-provoking. Please note that this document (or this recording of the presentation, as applicable) is provided for general information purposes only and does not constitute professional advice. No user should act on the basis of any material contained in the presentation or any of its supporting materials without obtaining proper professional advice specific to their situation.

Adapta has made reasonable efforts to ensure that the information provided is accurate and reliable, however no warranty is given regarding the accuracy or reliability of such information. All content is subject to change at any time and without notice.

The presentation may include references to specific products or services and/or links to other resources and websites. These references and links are provided for your convenience only and do not signify that Adapta endorses, approves or makes any representation or claim regarding the accuracy, copyright, compliance, legality, or any other aspects of the products, services resources or websites to which reference is made.

Additionally, the presentation may contain confidential and/or proprietary information, and must not be re-used or disclosed to third parties without the prior written approval of Adapta Consulting LLP.

If you would like further information or any advice regarding your own specific issues, then please do contact the Adapta team at hello@adaptaconsulting.co.uk