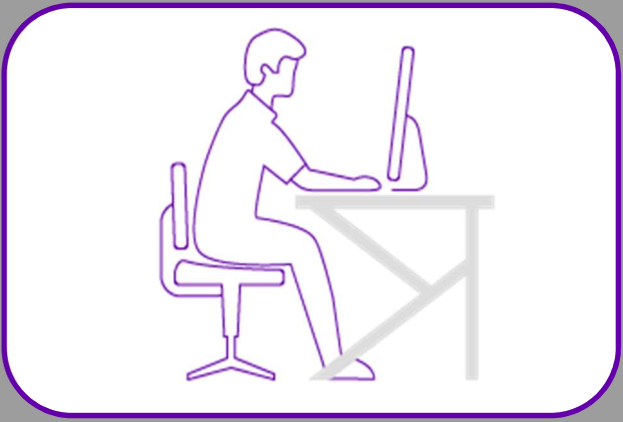
Public



PROTECTING BT

Our 3rd party supplier guide on email briefings

Guide: 1.1 3rd party

Owner: BT Security

This guide sets the basic controls for 3rd parties who on behalf of BT/EE are sending out email briefings to employees and BT/EE Customers.

Introduction

Phishing is BT/EE's #1 Security Risk. We're working hard to reduce the phishing risk. We've been giving our people lots of training on how to spot them. But, the more we utilise the services of 3rd parties to send out our briefings, the more difficult it is to our people to spot fraudulent emails. And if our colleagues think it's a phishing one they might well ignore it!

The aim of the recommendations below are to give the reader of the email briefing the confidence that the briefing is genuine and requires their full reading and follow-up action. It is not easy for email recipients to confirm that the communication is genuinely sent from a 3rd party as part of a service that is being provided to BT/EE by the 3rd party. Your BT/EE Stakeholder will advise you of the method to be used for you particular scope of work.

Who does this apply to?

This guide applies to 3rd parties carrying out work on behalf of BT/EE who design or configure systems that generate and distribute information for BT/EE through email. We may change this guide from time to time, subject to any agreed consultation processes.

Definition of terms:

Term	Explanation
must	This word, or the terms 'REQUIRED' or 'SHALL', means that the definition is an absolute requirement
must not	This phrase, or the phrase 'SHALL not', means that the definition is an absolute prohibition
may	This word, or the adjective 'OPTIONAL', means that an item is truly optional
should	This word, or the adjective 'RECOMMENDED', means that there be a valid reason in certain situations to ignore a specific item, but the implications will be fully understood and carefully assessed before choosing a different option.
should not	This phrase, or the phrase "NOT RECOMMENDED" means every effort will be made to meet the requirements of a control, but, it might not always be possible to avoid the action being described in all cases. Where a control can't be complied with the implications will be assessed and fully understood.

Scope

This document covers the minimum requirements to generate and distribute information for BT/EE through email.

What's included in this document?

1 Roles & Responsibilities.

BT/EE Stakeholders are responsible for making sure 3rd parties, are familiar and comply with the applicable requirements of this guide and any associated policies and standards.

2 Phishing.

BT Security provides important advice to alert employees to Phishing, we also have a CBT, 'Don't feed the Phish' with key advice on action to take when a phishing email is sent to their work email address.

However having this phishing awareness makes people aware of two key concerns, they are the origin of an email and the inclusion of links taking the user to external sites.

Therefore it is our preference is that the email should originate from a bt.com/ee.com domain rather than a 3rd party domain.

3 Email sender's address.

bt.com/ee.com

3.1 To provide confirmation of an official authorised email to the recipient.

3.2 The content of the briefing is determined solely by BT/EE.

3.3 The list of recipient email addresses are in the full control of BT/EE.

3.4 There is no need to upload lists of internal email addresses to a 3rd party.

It should be noted that provision of @bt.com/ee.com email address to 3rd parties is not generally acceptable as it provides 3rd parties with our brand without the same level of hygiene or controls that BT has in place.

Any 3rd party using @bt.com/ee.com will shortly be subject to DMARC restrictions which will inform the receiver to reject any mails not from an approved source.

3rd Party domain

3.5 BT/EE will need to approve 3rd party email address with verification available within the BT intranet e.g. the recipient can follow-up independently and check against a list of campaign related approved 3rd party email addresses.

3.6 The 3rd party must only use a BT/EE supplied distribution list.

3.7 If you are advised that there are problems receiving emails from your 3rd party address then notify your BT/EE Stakeholder and they will contact our 'Web Filter Team' to resolve.

4 Sender and Email header.

4.1 The "From" name and email address must identify the email sender.

4.2 The "Subject" line must be concise and relevant.

4.3 The sender must not include a visible email distribution list with multiple recipients.

4.4 The sender must not be using the 'bcc' field to email multiple recipients.

4.5 A postal address should be included in the content.

5 Links and Attachments.

NOTE: The concern on clicking on a link or opening an attachment is that an attacker will ask for information such as passwords and credit card details, or aim to download viruses, malware or ransomware onto your computer.

5.1 The email must not include attachments, question the BT/EE stakeholder if they do provide attachments.

5.2 If people are being asked to visit a website it should be SSL encrypted, DO NOT proceed if there is no encryption. You (or the BT/EE stakeholder if they are providing the text), should have a confirmation statement in the text confirming the URL is SSL encrypted.

5.3 You (or the BT/EE stakeholder if they are providing the text) should also contain a reminder to the reader to ensure that they check the address bar for 'https://' not 'http://' before they enter sensitive information.

5.4 Check that there is not a mismatched link where the URL recipient is directed to a URL that does not match the email URL: - (If the URL was provided by BT/EE check with BT/EE stakeholder if you believe there is an issue)

- To avoid suspicion you should not replace URLs with tracking redirect links.
- The URL should match the link typed into the message.

6 Body/Content.

NOTE: If you are providing the email content it is recommended that e-mails follow standard templates and style. (The following URL's are examples of syntax to be used and are not live links**)**

6.1 The body must be consistent with current branding guidelines, your BT/EE Stakeholder will be able to provide you with this. E.g. if you include a link BT Branding Site this could be mistaken for a 'phishing' email link, instead you would use www.btbranding.bt.com or https://www.btbranding.bt.com

6.2 Use personalisation, you must:-

- Include the first name of recipient at the top of the email.
- Add the name of person providing the briefing at the end of the email.
- Add the OUC of the person providing the briefing (this internal BT information is not normally known by scammers and fraudsters)

6.3 You must clearly explain the reason for the email.

6.4 You must indicate the authority allowing the email to be sent.

6.5 You should reference a briefing on a trusted website, your BT/EE stake holder will advise but for example a BT intranet page or 'BT Today' (BT/EEs employee newspaper).

6.6 Wording should be specific, don't include vague sentences.

6.7 Check spellings and grammar, as weaknesses of this type suggest a phishing email.

7 Customer Requirements' Management.

Example of good practice to ensure corporate consistency of email briefings: BT Group internal communications, should check the content of all briefings including all externally generated briefing emails before distribution to ensure that compliance with current branding requirement for internal email briefings, paying special attention to the style, presentation and wording.

The inclusion of a unique number in the email briefing is recommended against which to verify the communication (this number could be called Reference Authenticity Number / Anti-Phishing Number / Internal Authentication Number) –and would be valid for a limited duration e.g. 1 month.

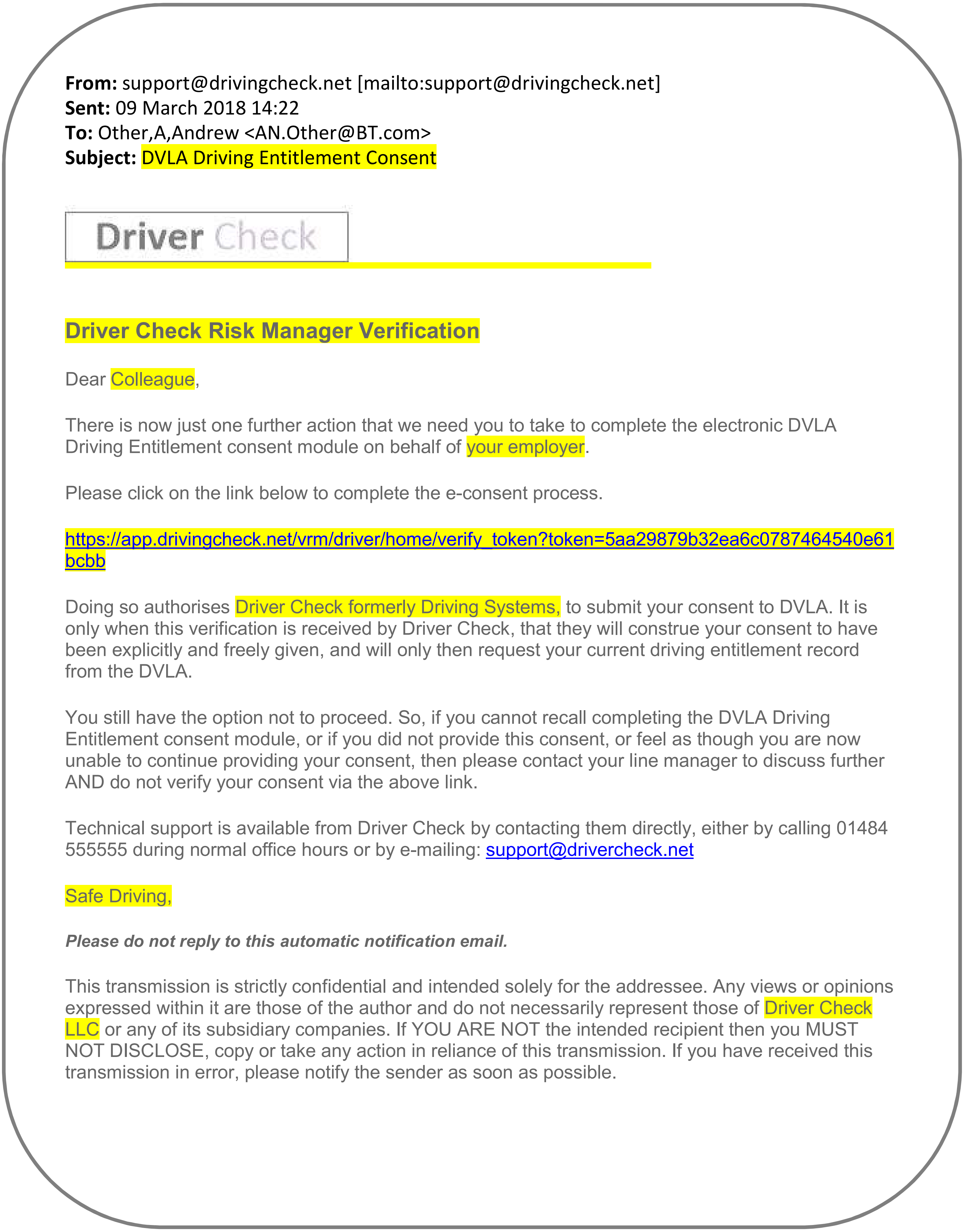
8 Examples of Email Briefings.

The following 3 email briefings are included:-

1. The first is a recent DVLA Driver Licence Check reminder which was considered by multiple recipients as potential 'Phishing' (page 7) - the phishing concerns are highlighted in 'yellow'.
2. The second is an improved version of this email (page 8) – the improvements are highlighted in 'green'.
3. A further recommended example email is the 'a Staff Rewards' reminder email (included as the third example).

(N.B email address, links and supplier names are fictitious)

8.1 Email received requesting DVLA Driver Licence Check.



From: support@drivingcheck.net [mailto:support@drivingcheck.net]
Sent: 09 March 2018 14:22
To: Other,A,Andrew <AN.Other@BT.com>
Subject: DVLA Driving Entitlement Consent

Driver Check

Driver Check Risk Manager Verification

Dear Colleague,

There is now just one further action that we need you to take to complete the electronic DVLA Driving Entitlement consent module on behalf of your employer.

Please click on the link below to complete the e-consent process.

https://app.drivingcheck.net/vrm/driver/home/verify_token?token=5aa29879b32ea6c0787464540e61bcbb

Doing so authorises Driver Check formerly Driving Systems, to submit your consent to DVLA. It is only when this verification is received by Driver Check, that they will construe your consent to have been explicitly and freely given, and will only then request your current driving entitlement record from the DVLA.

You still have the option not to proceed. So, if you cannot recall completing the DVLA Driving Entitlement consent module, or if you did not provide this consent, or feel as though you are now unable to continue providing your consent, then please contact your line manager to discuss further AND do not verify your consent via the above link.

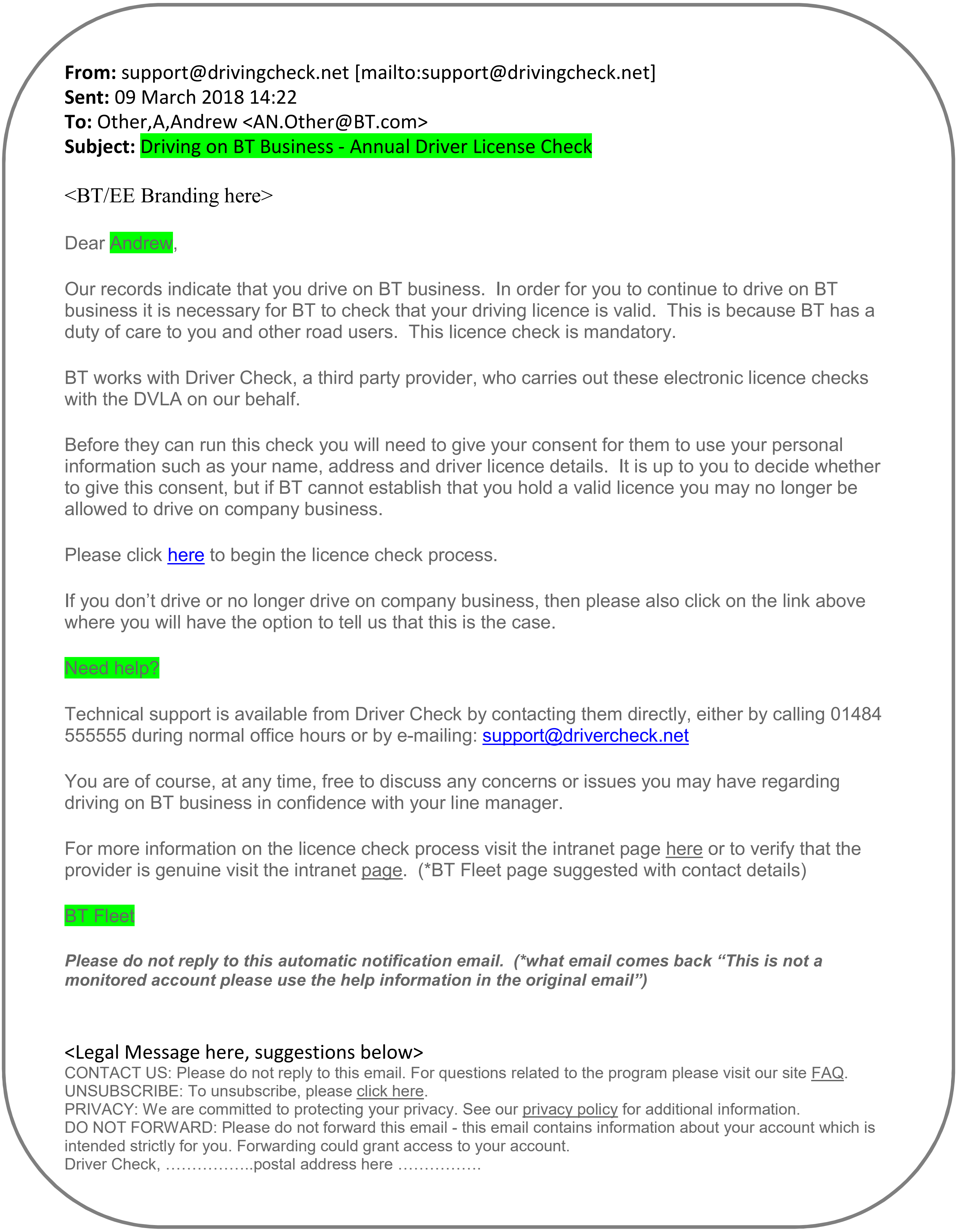
Technical support is available from Driver Check by contacting them directly, either by calling 01484 555555 during normal office hours or by e-mailing: support@drivercheck.net

Safe Driving,

Please do not reply to this automatic notification email.

This transmission is strictly confidential and intended solely for the addressee. Any views or opinions expressed within it are those of the author and do not necessarily represent those of Driver Check LLC or any of its subsidiary companies. If YOU ARE NOT the intended recipient then you MUST NOT DISCLOSE, copy or take any action in reliance of this transmission. If you have received this transmission in error, please notify the sender as soon as possible.

8.2 Improved email requesting DVLA Driver Licence Check.



From: support@drivingcheck.net [mailto:support@drivingcheck.net]
Sent: 09 March 2018 14:22
To: Other,A,Andrew <AN.Other@BT.com>
Subject: Driving on BT Business - Annual Driver License Check

<BT/EE Branding here>

Dear Andrew,

Our records indicate that you drive on BT business. In order for you to continue to drive on BT business it is necessary for BT to check that your driving licence is valid. This is because BT has a duty of care to you and other road users. This licence check is mandatory.

BT works with Driver Check, a third party provider, who carries out these electronic licence checks with the DVLA on our behalf.

Before they can run this check you will need to give your consent for them to use your personal information such as your name, address and driver licence details. It is up to you to decide whether to give this consent, but if BT cannot establish that you hold a valid licence you may no longer be allowed to drive on company business.

Please click here to begin the licence check process.

If you don’t drive or no longer drive on company business, then please also click on the link above where you will have the option to tell us that this is the case.

Need help?

Technical support is available from Driver Check by contacting them directly, either by calling 01484 555555 during normal office hours or by e-mailing: support@drivercheck.net

You are of course, at any time, free to discuss any concerns or issues you may have regarding driving on BT business in confidence with your line manager.

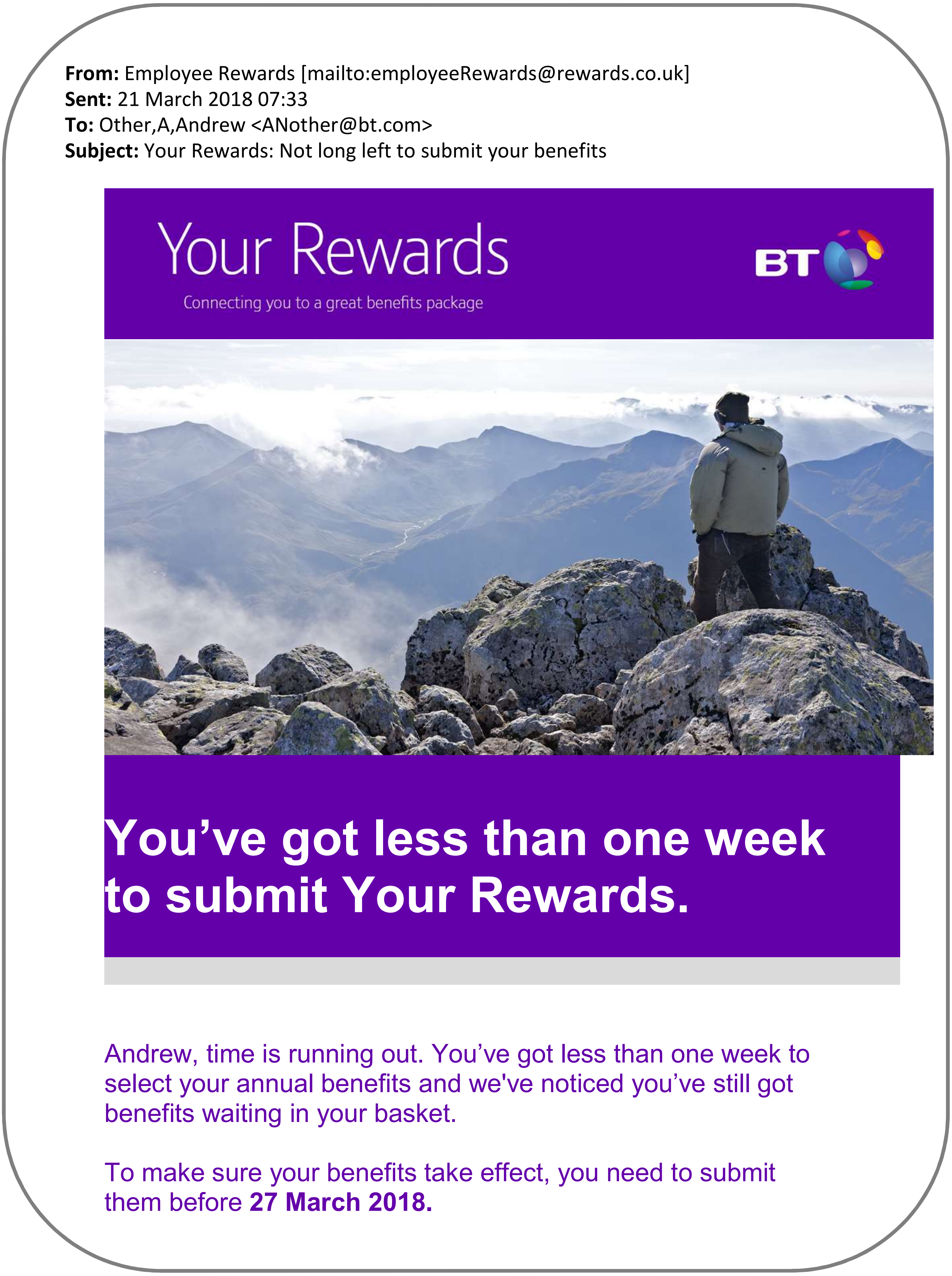
For more information on the licence check process visit the intranet page here or to verify that the provider is genuine visit the intranet page. (*BT Fleet page suggested with contact details)

BT Fleet

Please do not reply to this automatic notification email. (*what email comes back “This is not a monitored account please use the help information in the original email”)

<Legal Message here, suggestions below>
CONTACT US: Please do not reply to this email. For questions related to the program please visit our site FAQ.
UNSUBSCRIBE: To unsubscribe, please click here.
PRIVACY: We are committed to protecting your privacy. See our privacy policy for additional information.
DO NOT FORWARD: Please do not forward this email - this email contains information about your account which is intended strictly for you. Forwarding could grant access to your account.
Driver Check, ……………..postal address here …………….

8.3 Improved Your Rewards reminder email.



From: Employee Rewards [mailto:employeeRewards@rewards.co.uk]
Sent: 21 March 2018 07:33
To: Other,A,Andrew <ANother@bt.com>
Subject: Your Rewards: Not long left to submit your benefits

Your Rewards

Connecting you to a great benefits package

BT

You’ve got less than one week to submit Your Rewards.

Andrew, time is running out. You’ve got less than one week to select your annual benefits and we've noticed you’ve still got benefits waiting in your basket.

To make sure your benefits take effect, you need to submit them before **27 March 2018.**

Your Rewards Email continued........

Place your order from any online device:

Your Rewards is just like internet shopping. Simply add items to your basket and check them out. It's fully mobile too, giving you access whenever and wherever you want.

At work

- Link to Your Rewards here or from the BT HR Home or EE Reward Intranet pages.

At home or on your mobile device:

- Visit www.employee.rewards.co.uk
- Log in using your employee ID and password (the first time you log in, click 'I've forgotten my sign in details' and follow the prompts)
- Just a reminder that you shouldn't use your internal password on this, or any external site

Then:

- Click the 'Explore your benefits' icon
- Browse the benefits on offer
- Place your order before **27 March 2018**

Need help?

Your dedicated helpdesk is here to help with any questions. Get in touch by raising an online help ticket via Your Rewards and clicking the help icon, or over the phone on 0800 999 9999 (8.00am – 6.00pm, Mon to Fri).

9 Glossary.

Term	Explanation
CBT	Computer-based Training
CTIO	Chief Technology Information Officer.
DMARC	Domain-based Message Authentication, Reporting & Conformance. It is an email authentication protocol and is designed to give email domain owners the ability to protect their domain from unauthorised use, ie email spoofing.
DVLA	Driver Vehicle Licensing Agency.
Driver Check	Driver Check Online, covers driver risk assessments and annual driver licence check.
H&S	Health & Safety.
ISMS	Information Security Management System.
Phishing & Ransomware	• Phishing is an internet scam using deceptive emails to trick you into giving personal information or downloading malware! • Ransomware is an example of malware. It stops you accessing data on your machine until you've paid a ransom. • Other forms of phishing are whaling and spear phishing. These target specific groups of people.

10 Change History.

Version no	Date	Change made by	Brief details of change
1.0 Draft	18/07/19	David Rabone	3rd Party Version Created
1.1 Draft	31/07/19	Karen Tanner	Anonymisation.
1.0 Issued	01/08/19	Karen Tanner	Approved by BT Version Owner.
1.1 Issued	14/01/20	Karen Tanner	Change data classification for this document.

11 Document Sign off.

Name	Role	Date
David Rabone	BT Version Owner	01/08/19
David Rabone	BT Version Owner	14/01/20

12 Compliance.

If you behave in a way that's inconsistent with this guide or any other policy or standard, we may terminate the arrangements we have with you for your services.

13 Ownership & Confidentiality.

This document must not be shared with any other third party without the written consent of BT. This guide and any associated documentation remains the property of BT and must be returned if requested.