



CATCH THE PHISH

Don't take the bait

CPNI

Centre for the Protection
of National Infrastructure



DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

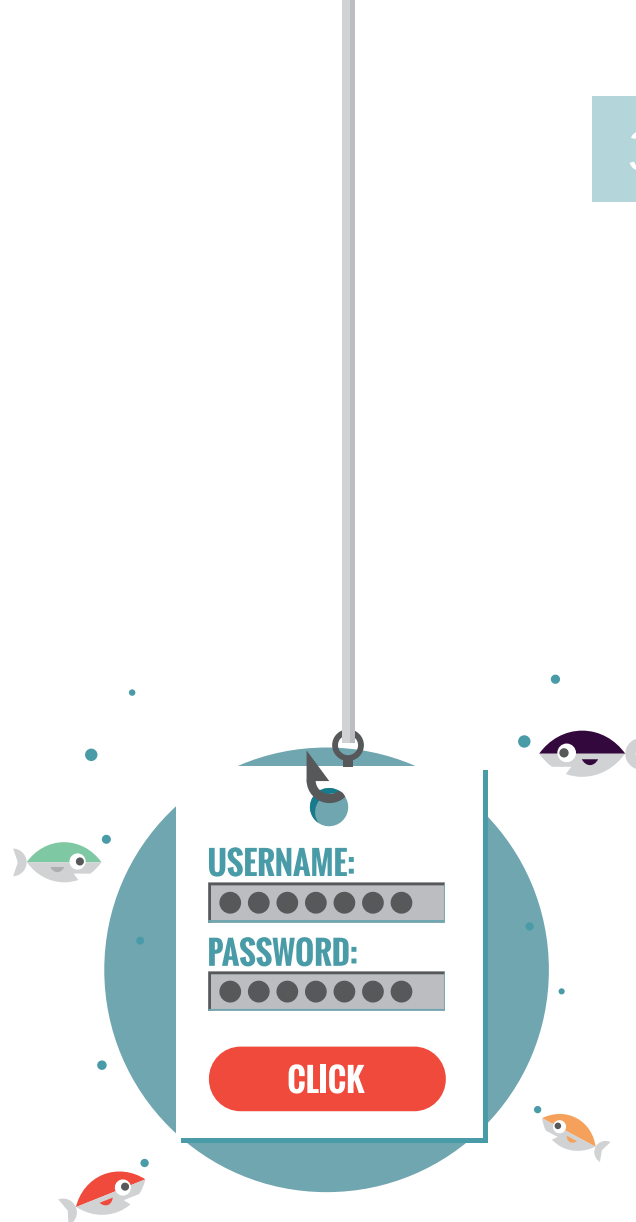
© Crown Copyright 2017

INTRODUCTION

This quiz has eight example messages. For each, you must decide whether you think it is genuine by selecting 'real' or an example of phishing by selecting 'phish'.

The answers are provided towards the back of this booklet. Give yourself one point for each correct answer. Turn to page 21 to discover what your results mean.

HINT: CPNI's 'Don't Take The Bait!' animation and infographic provides information that may help you to spot phishing attempts.



WHAT IS PHISHING?

Phishing is when an attacker looks to exploit a user in order to bypass security measures, via an electronic communication, e.g. an email.

WHAT IS SPEAR PHISHING?

Spear phishing is a targeted type of phishing. An attacker finds out information about an individual which allows them to tailor their attacks and appear trustworthy in an electronic communication.

EXAMPLE 1

New Message — ↗ ✕

From Home Foods ([do not reply@points.homefoods.co.uk](mailto:do_not_reply@points.homefoods.co.uk))

Date Weds 29 March 2017 12:25:55 +0200

Subject We are giving away free Home Foods gifts


Dear Luke,

This spring, Home Foods are celebrating our 10th anniversary. In celebration of this we are giving away a limited number of free Home Foods gifts - all you have to do is register your details and tell us your favourite Home Food store!

To register for your free gifts now, click [HERE](#).


Sincerely,


Home Food Customer Service



Copyright © 2016 Home Foods. All Rights Reserved.

Reply 🔗 📎 📧 📄 🔗

 **REAL**

 **PHISH**

EXAMPLE 2

New Message — ↗ ✕

From Justin.williams@communicationslounge.com

To BarbaraW@energyorg.co.uk

Subject Design files as requested

Message ID: CSAXDLodNTJkyuX9LCyzz3LBTZTcsq1=NamdfSQ@mail.com


This message has been held to queue "Unknown Filetype"


Reasons for this are indicated below.

Attachment 3 "BOOKLET_FINAL.indd", identified as '(Minimum strength) (strength Implied:0)': The attachment is of an unspecified data type 'unidentified'.

Please contact the IT Service Desk for further assistance.

Reply 🔗 📎 🔄 ₤ 📄 ↔ 🔍

 **REAL**

 **PHISH**

EXAMPLE 3

New Message — ↗ ✕

From "Alpha Express" AlphaExpress@welcome.aexp.com

Subject Security Concern on Your Alpha Express

Dear Customer:

We are writing to you because we need to speak with you **regarding a security concern** on your account. Our records indicate that you recently used your Alpha Express card on April 29, 2017.

For your security, new charges on the accounts listed above may be declined. If applicable, you should advise any Additional Card Member(s) on your account that their new charges may also be declined.

To secure your account, please log in at:

<http://alphaexpress.com>


Your prompt response regarding this matter is appreciated.


Sincerely,

Alpha Express Identity Protection Team

Please do not reply to this e-mail. This customer service e-mail was sent to you by Alpha Express. You may receive customer service e-mails even if you have unsubscribed from marketing e-mails from Alpha Express.


Reply 🔗 📎 📧 📧 🔗 📧

 **REAL**

 **PHISH**

EXAMPLE 4

New Message



On 12 May, 2017, you removed a card ending 356 from your NetworkPay account.

Any payments you authorised on the card before 13 May will be completed; however, no new payments will be processed on this card.




Didn't make this update?

If you didn't make this change, log into your NetworkPay account and review your information as soon as possible. If you notice any unusual activity, please contact our help centre immediately. The details are available on our website.

Thanks,

NetworkPay

Reply



REAL

PHISH

EXAMPLE 5

New Message — ↗ ✕

From Federal Trade Council [mailto: ftc.ivRY9@ftcc.gov.uk]

Date 03 January 2017 15:07

To Jones, Amal

Subject CONSUMER COMPLAINT NOTIFICATION

Dear Amal,

This notification has been sent to you because we have received a consumer complaint, claiming that your company is violating the CCPA (Consumer Credit Protection Act).

According to our policy we have initiated a formal investigation before taking legal action.

You can download the document containing the complaint and the plaintiff contact information from:

https://ftcc.gov/download.aspx?complaint_id=4306534


Note that Adobe Reader must be installed on your computer.


Please take a moment to read the bolded section in the complaint, regarding the CCPA complaint.

Regards,

Federal Trade Council

Reply 🔗 📎 📄 🌐 📧

 **REAL**

 **PHISH**

EXAMPLE 6

New Message — ↗ ✕

From fayU16@email.com

Date 19 June 2017 13:20


To Anna King

Hi Anna,


I saw your recent presentation at the Green Energy UK conference. I have attached a new research paper that you may find interesting.


It hasn't yet been published!

Regards,

 [Report green energy.docx](#)

Reply 🔍 📎 🔄 £ 📄 🔗 🌐

 **REAL**

 **PHISH**

EXAMPLE 7

New Message — ↗ ✕

From "HR Pay and Reward" HRPR@watercompany.co.uk

Subject HR Latest- PAY DEAL 17/18

Dear employee,

We are writing to you following the conclusion of the provisional negotiations regarding pay increases for the financial year 17/18.

Given the current financial climate we are pleased to announce that we have successfully negotiated improved salary ranges for each grade.

For further details of the new ranges and for information as to how these changes may affect you, please refer to the HR pages.

Kind regards,


HR Pay and Reward


Northington House Estate

@watercompany

<http://intranet/HRPR>

Reply 🔗 📎 📄 🌐 🔗 🔗

 **REAL**

 **PHISH**

EXAMPLE 8

New Message — ↗ ✕

From ops_invoice@adx.ng

To accounts@thetransportcompany.co.uk

Attachments [Inv_#387562.ZIP\(82kb\)](#)

Dear accounts department,

Please find attached your invoice for review. If you have any queries please contact your ADX team on the number **provided in your invoice**.


Important: do not reply to this email as this inbox is not monitored.


Please pay this invoice at your earliest convenience to avoid additional charges.

Thank you for choosing ADX,

ADX Team

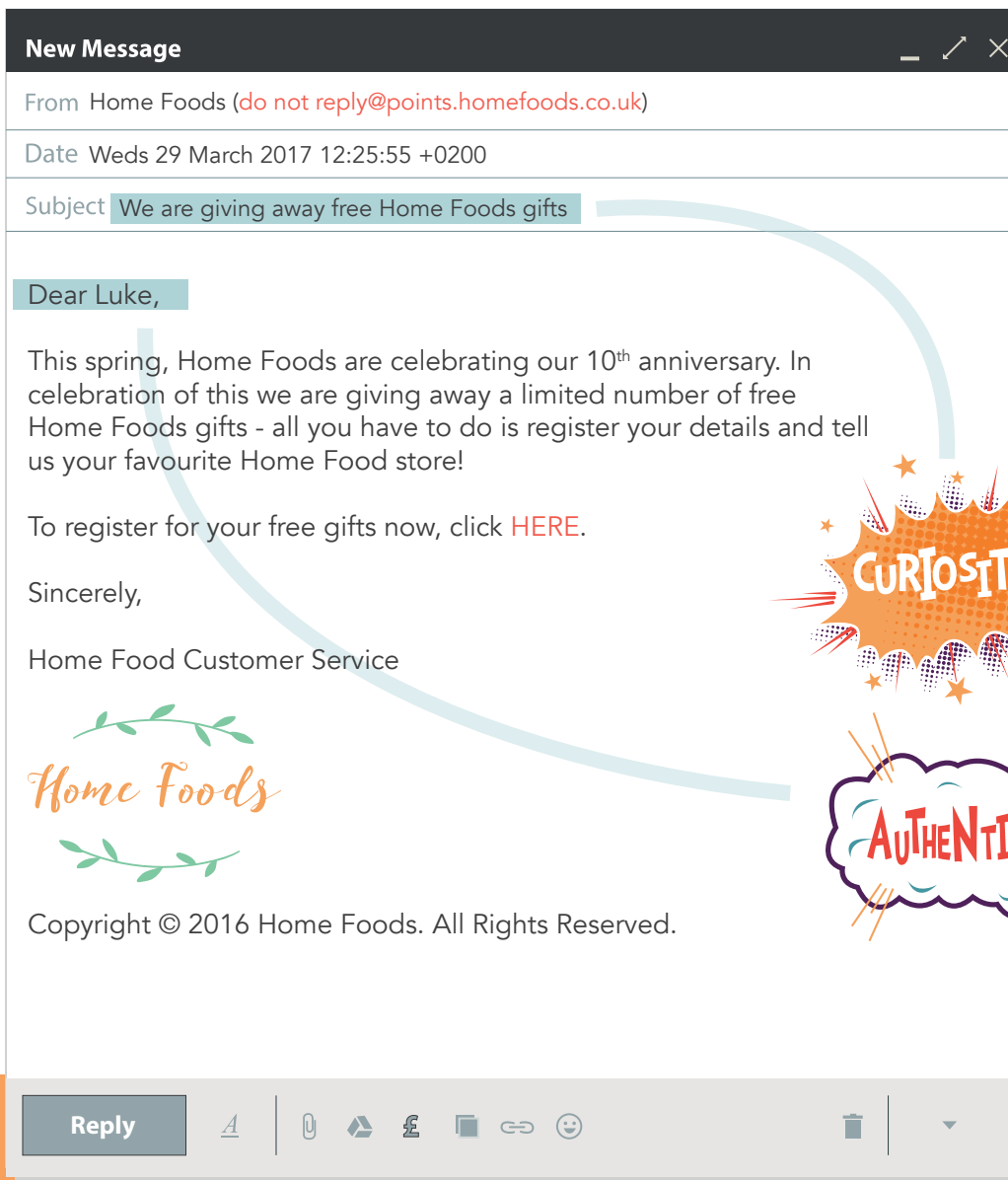
Reply 🔗 📎 🌐 📄 🔗 🔗

 **REAL**

 **PHISH**

TURN THE PAGE FOR QUIZ RESULTS!

EXAMPLE 1



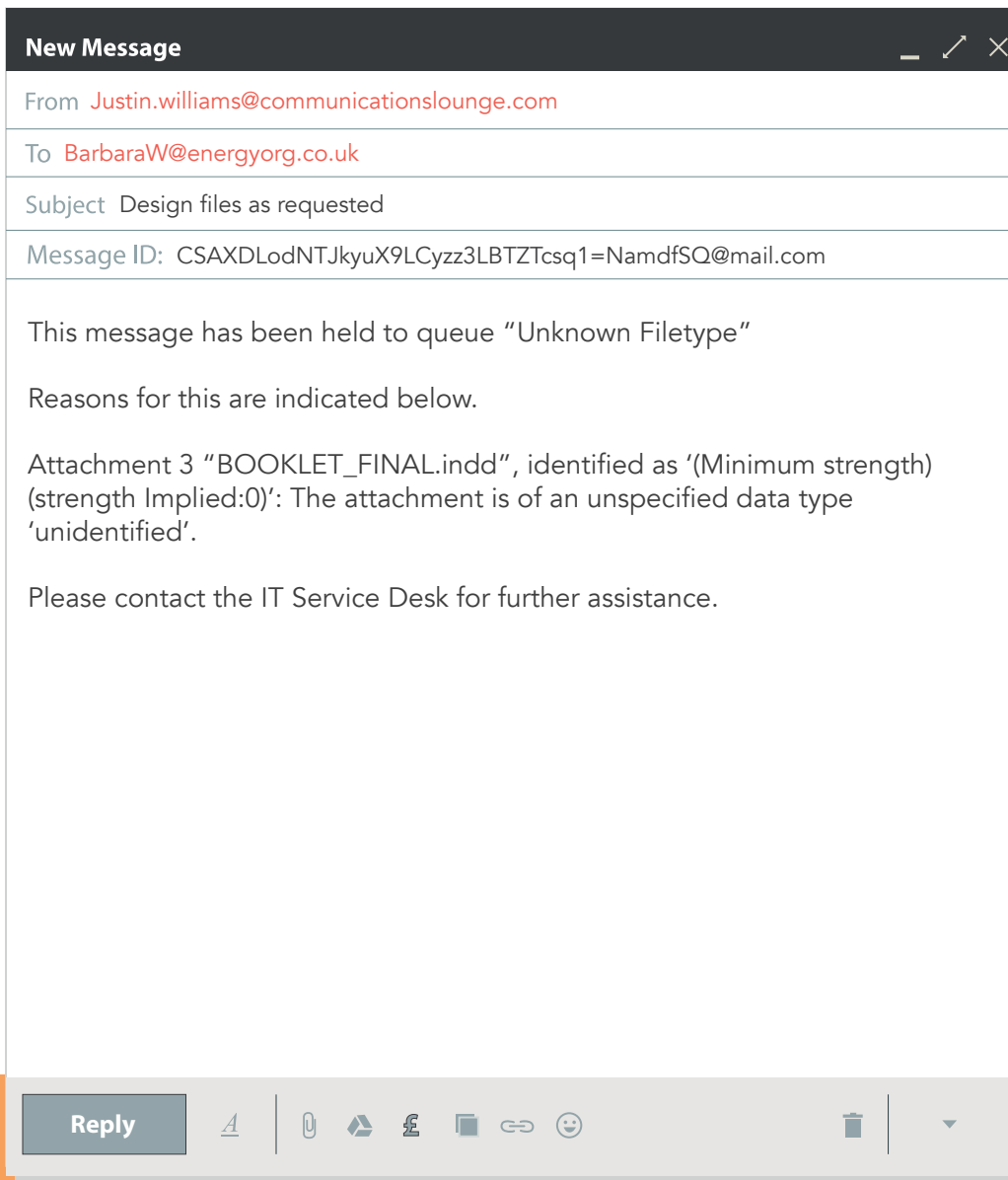
The phisher may have details that the user is a customer of Home Foods, and so the email may appear authentic e.g. addressed to the user by name, including well known logos.

Phishers may use images and details of popular events (e.g. sports) and references to reward (e.g. free gifts) to

encourage a sense of curiosity to click the link.

The misspelling of 'Home Food' in the sign-off also suggests something might be amiss, though do be wary that spelling and typographical mistakes occur in real emails, too.

EXAMPLE 2

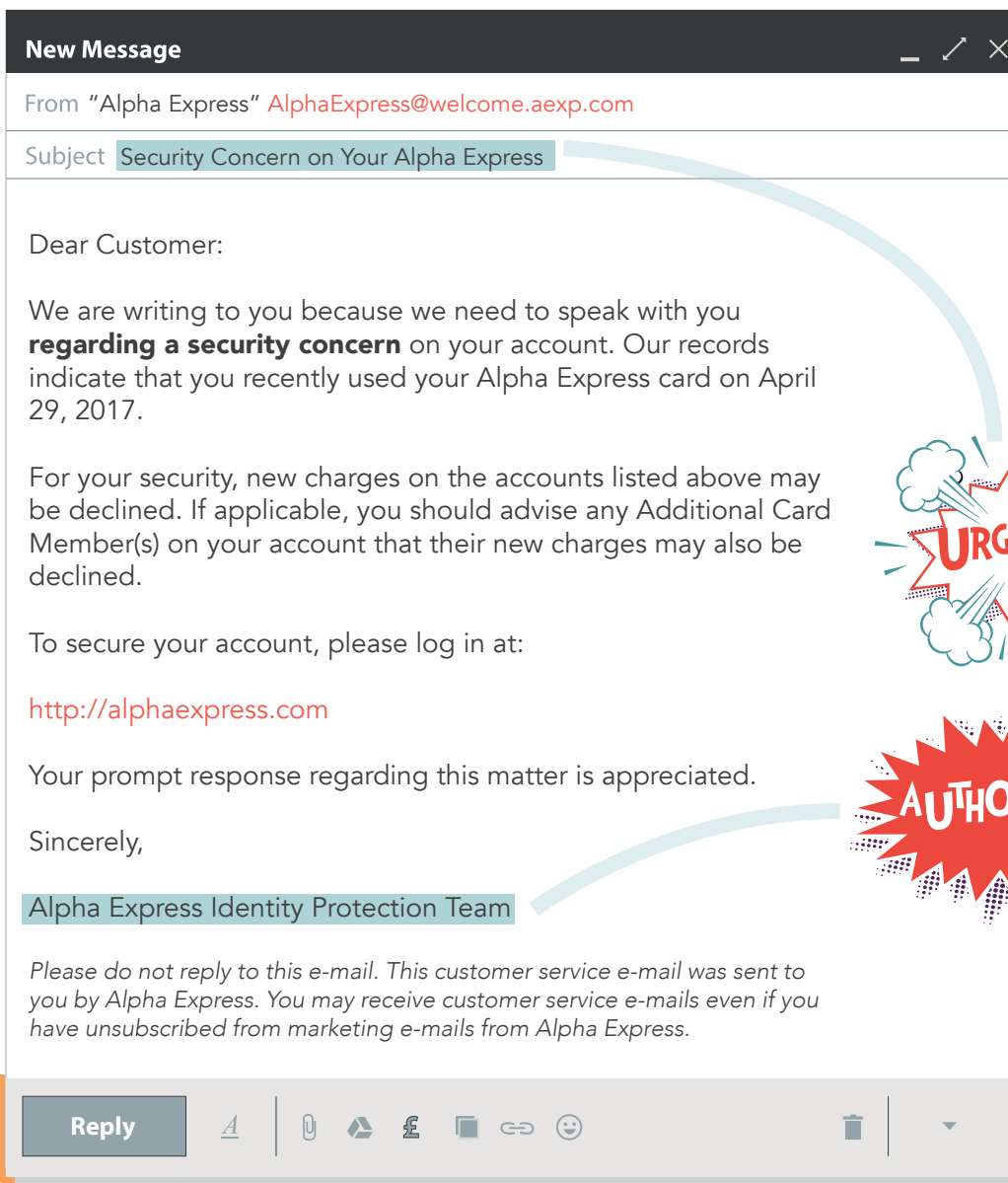


This is an automated notification that an attachment meant for the user has not passed the technical controls of the email system, e.g. it is a banned file type.

The user is not being encouraged to respond to the message directly. This may be an indication that a message is not suspicious, although more sophisticated approaches may only ask a user to respond after a series of communications.

The correct action here would be for the user to consider whether the sender is known to them and whether they were expecting the attachment. The user could contact their IT service desk (using the organisation's usual method) to check whether the attachment can be retrieved securely.

EXAMPLE 3



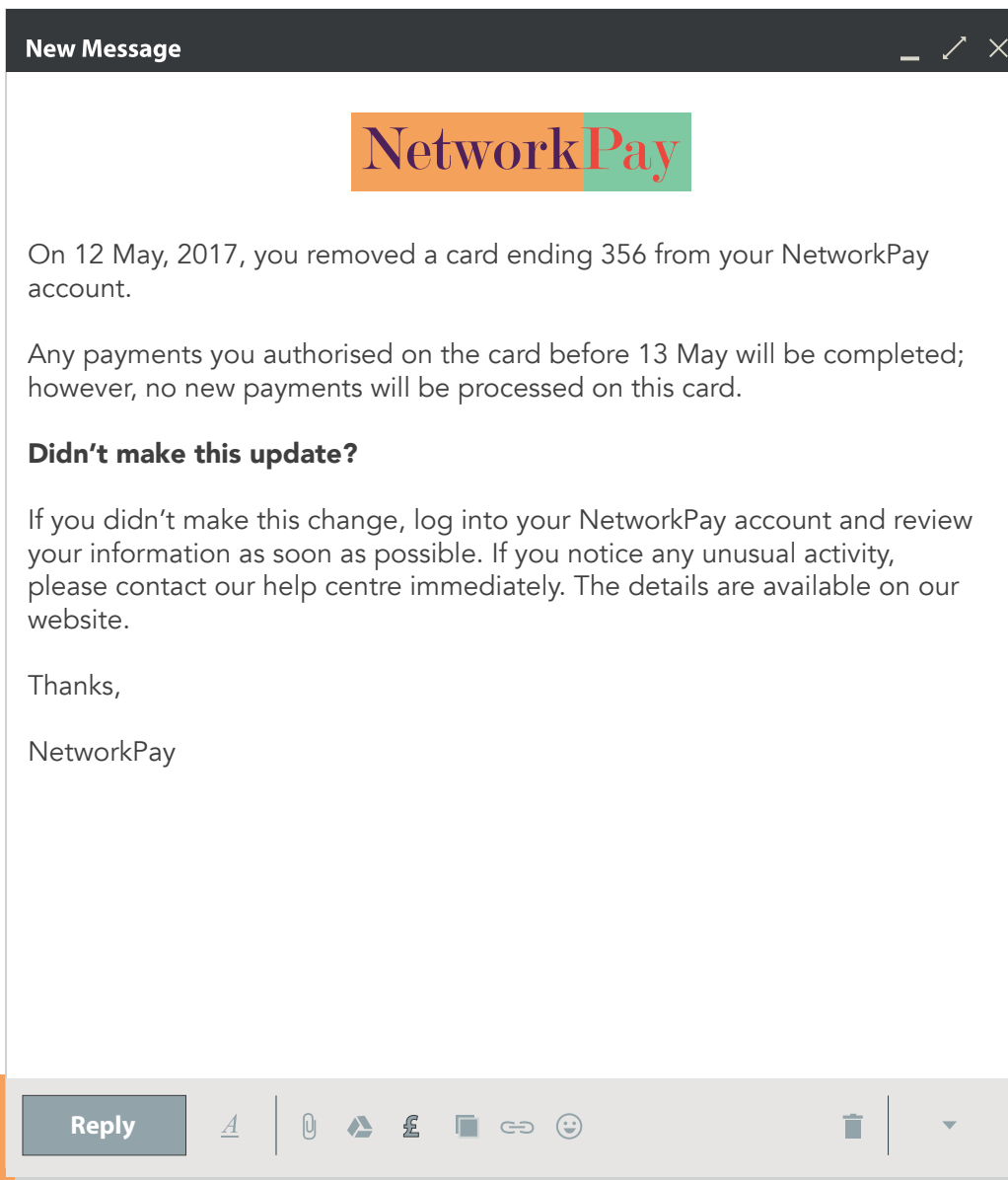
The 'Alpha Express Identity Protection Team' suggests authority with the subject; the user may feel that they have a lower understanding of identity protection.

The user may feel pressured to respond quickly to the email to reduce negative implications, e.g. declined charges or loss of access to their credit card.

The phisher has provided a way out for the user, by following the link to 'secure their account'.

Busy or distracted users, or those unfamiliar with the way their card provider usually communicates, may be tempted to click the link.

EXAMPLE 4

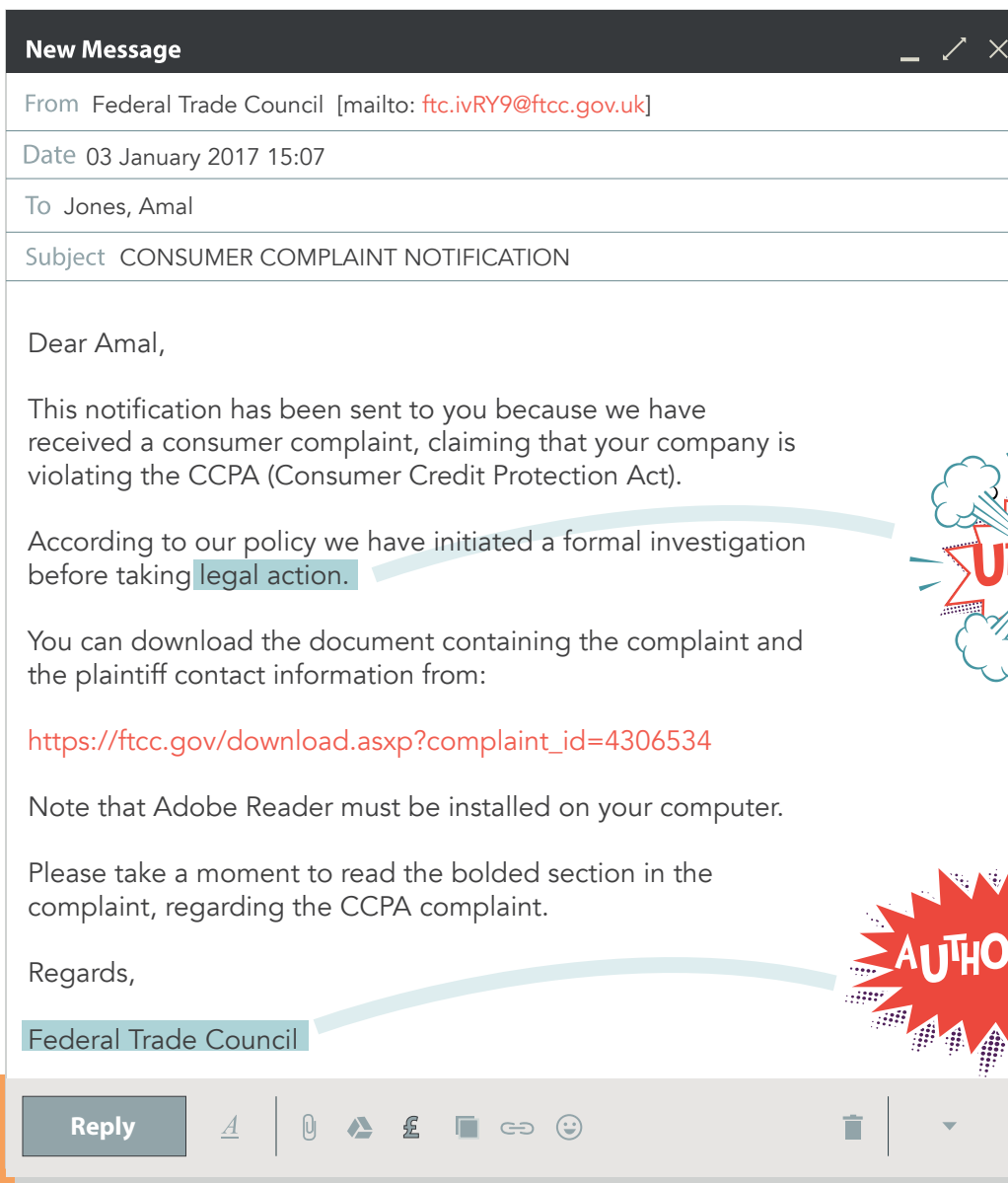


This email is an example of how a genuine company may notify a customer that there have been changes to their account. The message does not request that the customer responds by clicking a link or opening an attachment. It makes no request for the customer to provide personal details to the email

sender directly, e.g. account numbers or passwords.

If the user is suspicious they are able to visit the usual website of the company and do their own research rather than following a link suggested in the email, which could be spoofed.

EXAMPLE 5



The email purports to be from the 'Federal Trade Council', attempting to make the email appear authoritative. It appears to refer to a US organisation, but it wouldn't make sense for them to have a UK government email address!

Some of the language in the email is more commonly associated with the US legal context, e.g. 'violating' and 'plaintiffs'.

The email uses fear appeals, e.g. suggesting legal action may be imminent to encourage urgent action by the receiver.

The time and date that this phishing email was received is interesting. How alert might you feel when working through your email inbox at 3pm on the first working day of the year?

EXAMPLE 6



This message is an example of spear phishing; it a targeted attempt to compromise the user.

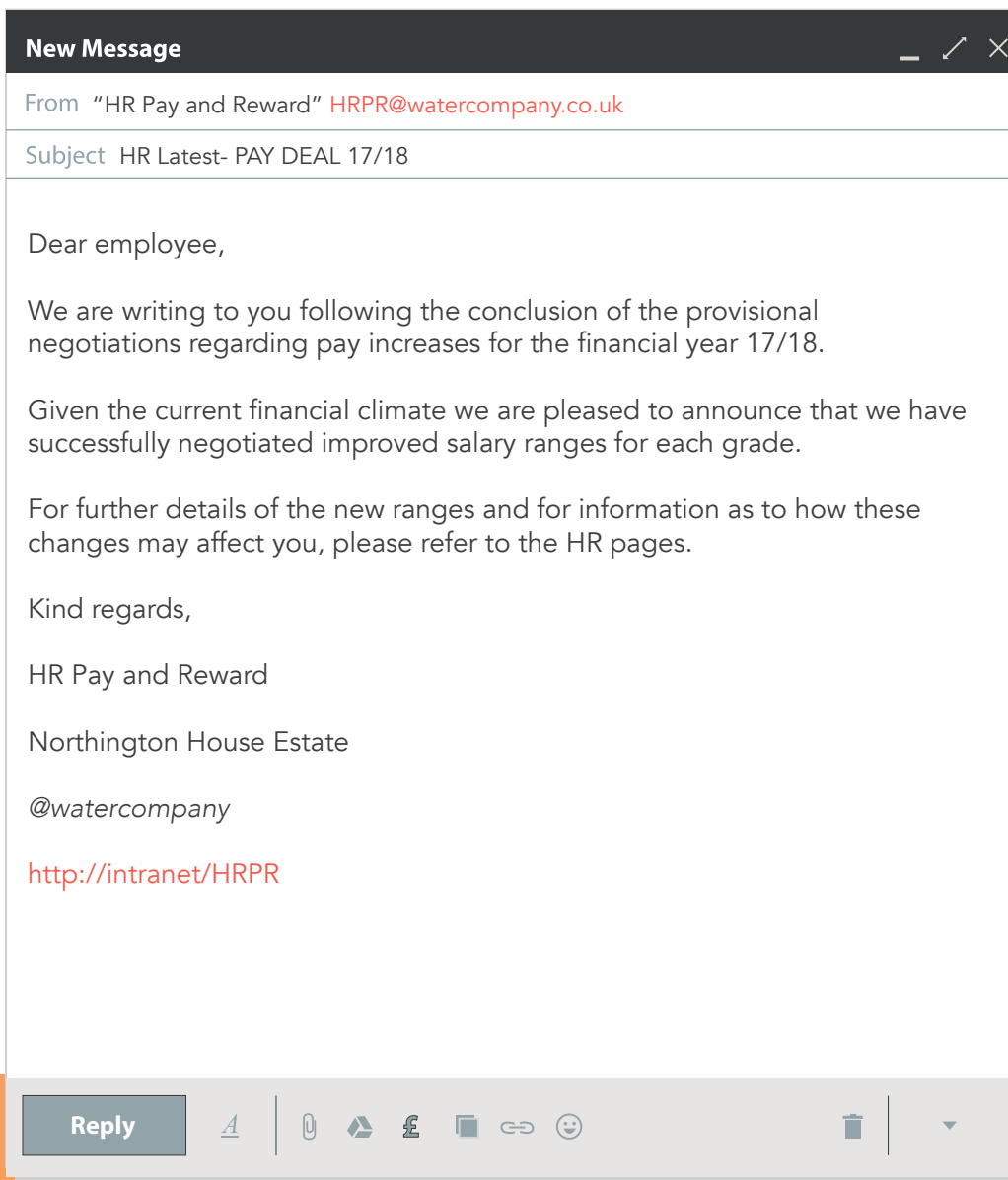
It may appear convincing as it includes authentic details relating to the user, e.g the conference presentation. But the phisher has found this information online.

The sender has not provided details of their name or organisation

The phisher entices the user to open the attachment by invoking curiosity- the appeal of getting early knowledge of new research in their specialist area.

It can be tricky to identify more sophisticated and tailored emails. Report anything suspicious to IT, even if you think you might have taken the bait.

EXAMPLE 7

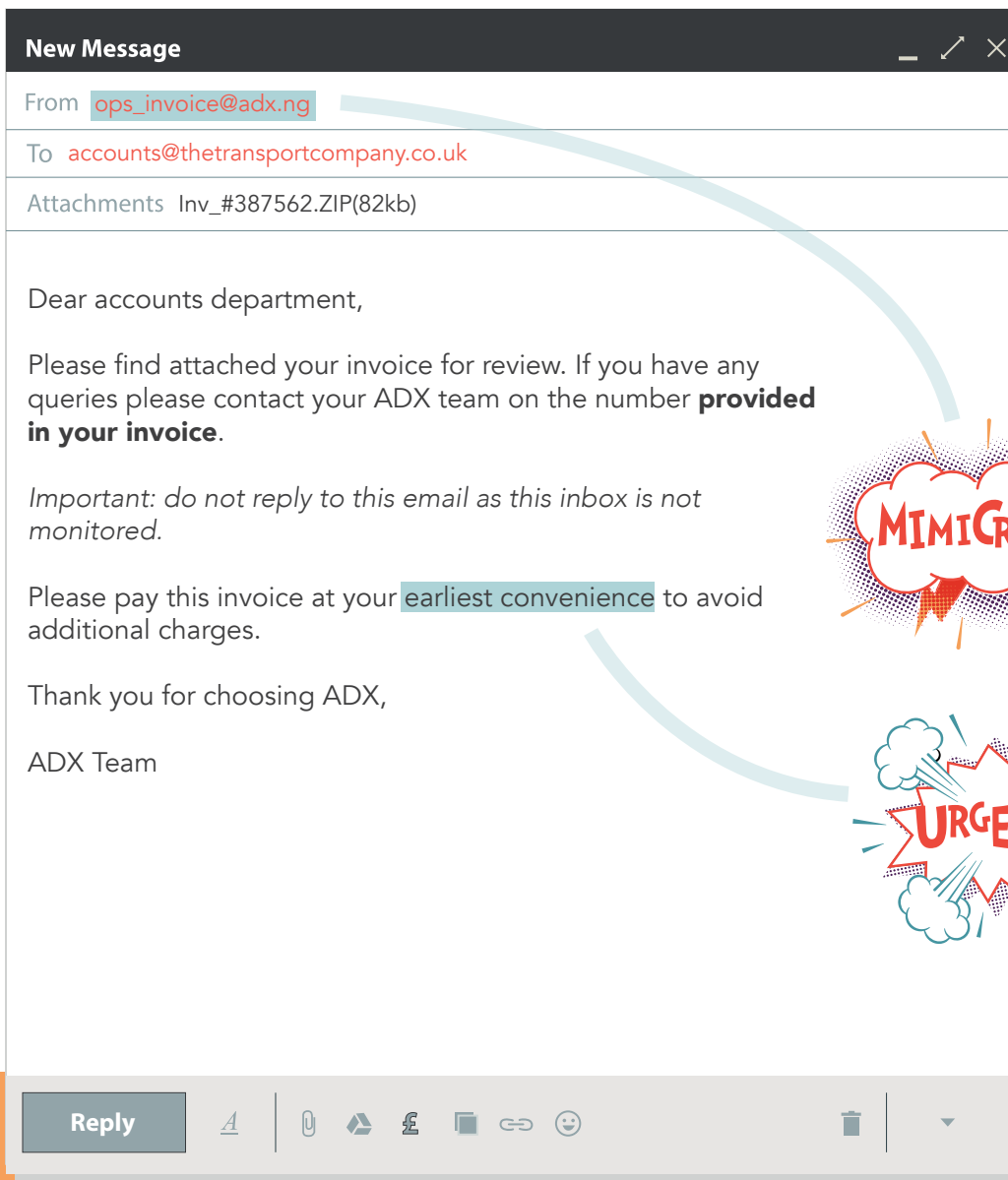


This is a real email, from the organisation's HR team.

The user can choose to follow up with their own independent research on the organisation's intranet if required.

Errors such as spelling and typographical mistakes are common in genuine emails. As phishing attempts have become increasingly sophisticated, these are not reliable cues.

EXAMPLE 8



This is an example of an invoice phishing scam. This message has been sent to an accounts employee, and it is intended to mimic the type of emails they would expect to receive. The employee is put under pressure to respond urgently to avoid the accrual of a financial penalty.

This organisation may open the malicious attachment which could have consequences such as facilitating a cyber-attack. A busy employee may seek to action the invoice before validating whether it is real.

Think before you click. Are you expecting the email? Do you know the sender?

SCORING

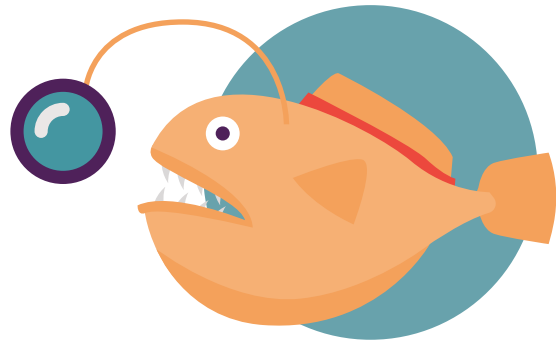
NINJA PHISH 7-8

Wow, you are skilled in identifying even the trickiest of phishing scams! You successfully tread the line between being wary of phishing scams and spotting real messages that require your response. But be aware that phishers are out there creating ever more sophisticated scams to fool even the most experienced users. Report anything suspicious to IT.



DETECTIVE PHISH 5-6

You are pretty good at identifying phishing scams! If you are in doubt that an electronic communication you receive is genuine you can seek advice from colleagues or your IT department. It pays to think before you click; trust your judgement if you think something may be suspicious.



PUZZLED PHISH 0-4

Not to worry! Identifying phishing scams can be difficult because phishers create sophisticated messages. Speak to your colleagues, manager or your organisation's IT department if you feel you need further support or training in identifying phishing scams.



Look out for CPNI's 'Don't Take The Bait!' animation and infographic for tips on how to spot phishing attempts.

ANIMATION



INFOGRAPHIC

