Protecting against mail/web scams

An example-based tutorial

Protecting against scams – a ‘how to’ session

'I feel like a total failure': Pensioner devastated after losing over £75k savings in scam

EXCLUSIVE: Over the past five years, an approximate total of £1.7 billion has been lost in fraud cases involving victims aged 65 or older - resulting in a loss of approximately £1.2million each day.

Protecting against scams – a ‘how to’ session

- Being the victim of a scam is a distressing experience, which at the high end of the spectrum of fraud losses, can be life changing
- There is much information available (which will be listed later), but generally it is focussed on **‘what’** to avoid e.g. ‘fake’ e-mails
- But how do you recognise a ‘fake’ e-mail ? People lose money because ‘professional’ scammers can be very ‘good’ at what they do.
- This session will attempt to help **‘how to’** recognise scams generally
- However, we strongly recommend you to study the excellent guide ‘Avoiding scams’ issued by ageUK –it can be downloaded here
- https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/scams-guide/

Types of scams

- A scammer first has to establish contact with you in some way, and then perpetrate the fraud. There are potentially four types of approach:-

- **'one shot' scams:** Probably the most common, contact can be established by knocking on the door, sending postal mail, contact by phone, and (the most common) contact via e-mail or web site.

- **Relationship scams:** Generally, contact is made via a web dating site. The scammer seeks to establish a close relationship over time, and then seeks to extract money, often in a series of acts.

- **Identity theft:** These scams are effected by the perpetrator impersonating the victim, and then fraudulently opening accounts etc and entering into contracts for goods.

- **Investment / pension scams:** This type of scam is likely to result in by far the greatest loss of any type. The victim is typically persuaded to transfer pension or savings assets to an apparently sound company, but which is in fact a front for the scammer.

Types of scams

- This session will focus on ‘one shot’ scams, and (maybe) touch towards the end on Investment scams

- The majority of ‘one shot’ scams are via e-mail or the web, as the scammer can cover more victims and can operate from another country The examples in this session will be about this route into your pocket.

- Relationship scams are probably the most vile, since they may have a personal emotional effect far worse than simply losing money. We won’t cover these in this session.

- Identity theft is different from the other scams, because the scammer does not actually want to make contact with you; the goal is to hide the activities from you. This is a separate topic and won’t be addressed here.

- Investment scams are complex because they require positive and knowing cooperation by the victim, who is duped into making a change. Further, there are such a large variety of investments types, we can’t cover them here. However, there are some common ground rules, and these will be described.

E-mail and web scams

- The general principles here apply to approaches by phone, letter or (less common these days, knocking on the door.

- The internet scammer wants you to click on a link / attachment to

    - provide personal data (bank account details, passwords etc)
    - download a dangerous attachment
    - pay money to release a delivery
    - Buy a dubious product
    - ‘invest’ in a worthless scheme
    - believe that someone really owe you $25,000,000

- However, they tend to have a common form, which should ring alarm bells

- **Note: if you are expecting a mail, it comes from a known sender, and can verify the content as being expected or genuine, then it’s probably ok !**

- So now for some examples, for you to become a scam recognition master !

On of the oldest scams – the 'Nigerian'

From: Mr. Kennedy Uzoka <no-reply@ng.tn>
Sent: 15 October 2023 14:01
To: Recipients
Subject: KINDLY RESPOND.REF.GMAK/37

UNITED BANK FOR AFRICA - AFRICA'S GLOBAL BANK HEAD OFFICE ADDRESS UBA HOUSE
57 MARINA P.O. BOX 2406 LAGOS NIGERIA
phone no: +234 706 815 3659
FAX: 234 674 478 8273

I Am Mr.Kennedy Uzoka the director cash processing united bank for African the international monetary fund (I.M.F.) in conjunction with Organization of African Unity (A.U) is compensating all the scam victims with $1.500.000.00USD and your email address was found in the scam victim's, the united bank for African and Federal Reserve Bank has been mandated by the (I.M.F) to pay your compensation ($1.500, 000.00USD) in cash through means of diplomatic courier service hand delivery.

Take note that Three thousand united states dollars (usd$3,000) have been mapped out for all expenses in taxes and other documents that matters. Therefore, kindly forward your home address, direct phone number to the below email address mrkdyuzkub56@gmail.com

Regards,
Mr.Kennedy Uzoka
Director cash processing unit
United bank of Africa. (U.B.A).
Phone no: +234 706 815 3659

One of the oldest scams – the 'Nigerian'

From: Mr. Kennedy Uzoka <no-reply@ng.tn>
Sent: 15 October 2023 14:01
To: Recipients
Subject: KINDLY RESPOND.REF.GMAK/37

UNITED BANK FOR AFRICA - AFRICA'S GLOBAL BANK HEAD OFFICE ADDRESS UBA HOUSE
57 MARINA P.O. BOX 2406 LAGOS NIGERIA
phone no: +234 706 815 3659
FAX: 234 674 478 8273

I Am Mr.Kennedy Uzoka the director cash processing united bank for African the international monetary fund (I.M.F.) in conjunction with Organization of African Unity (A.U) is compensating all the scam victims with $1.500.000.00USD and your email address was found in the scam victim's, the united bank for African and Federal Reserve Bank has been mandated by the (I.M.F) to pay your compensation ($1.500, 000.00USD) in cash through means of diplomatic courier service hand delivery.

Take note that Three thousand united states dollars (usd$3,000) have been mapped out for all expenses in taxes and other documents that matters. Therefore, kindly forward your home address, direct phone number to the below email address mrkdyuzkub56@gmail.com

Regards,
Mr.Kennedy Uzoka
Director cash processing unit
United bank of Africa. (U.B.A).
Phone no: +234 706 815 3659

One of the oldest scams – the 'Nigerian'

- You won't see many of these, but it was a very early scam, which illustrates some important points. Nigerian scammers promising large rewards were early 'pioneers'

- The 'clues'

  - 'From' address not connected with apparent sender, and 'no-reply'
  - 'To' address not specific ; 'To' addresses which are 'recipients', 'me', and blank should put your **scam-o-meter** ("s-o-m") to 'warning'.
  - Promise of a big reward (the greed motive for a reply)
  - The scammers 'stupid filter' – mention of an up-front payment of $3,000. This is an 'advance fee' scam (i.e. take the money and run) , and we'll see this again.
  - Private return e-mail address, not the apparent sender. Your s-o-m starts to beep.

- On the face of it, this is a pretty dumb attempt at scamming because it's so obviously crooked. In actual fact, it's very clever, as will be explained.

Running scam-o-meter warning flags list

- Unconnected with apparent sender ‘From’ address
- Non-specific ‘To’ address ‘undisclosed-recipients’ / ‘recipients’ / ‘me’ / blank
- Promise of reward / benefit (‘greed’) or loss / penalty (‘fear’)
- Unconnected mail reply address with apparent sender (+2 pips for gmail)

A Natwest mail

From: natWest <sylvie-manuella1942880770@ac-versailles.fr>
Sent: 07 November 2023 14:01
To: undisclosed-recipients:
Subject: Fwd:(1)Notice!

Dear customer,

Our system recognizes that you have not yet activated our new NatWest Mobile security service, so you can easily control your NatWest account:

Do this or negative outcome

The Natwest Card Reader will disappear at the end of 2023 because it takes a long time to respond to online transactions. Use the application “NatWest MOBILE” security to control your instant internet purchases without wasting time.

Click a link or button

Activate “Natwest Mobile” by following the instructions.

1. Log in with your bank details.
2. To confirm your update use your Natwest Card Reader.

Sincerely.

A Natwest mail – don't click risky links !

- Scammers will seek to use the promise of the bargain or threat of a loss to click a link or press a button. Never do this unless you are ***absolutely sure*** that the mail or web page is completely genuine.

- Clicking a bad link can

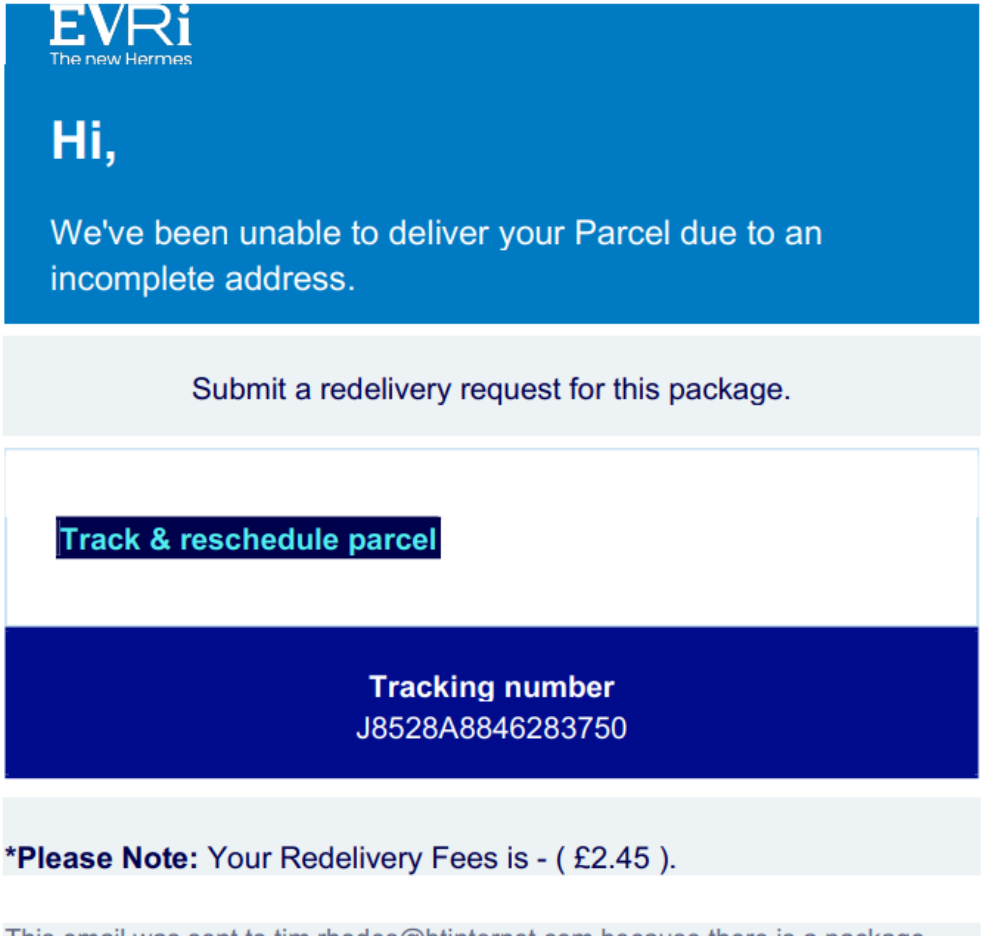
  - download malicious material (virus, spyware) onto your device
  - take you to a web page which asks for sensitive information
  - reveal information about your device and e-mail to them

- Tip no 1: If you hover your mouse pointer over a link (but don't click!!!) it will often show you where the link points to

  - Which is obviously NOT Natwest !

The delivery ‘advance fee’ scam

From: Evri ® <geraldine.middleton@btconnect.com>
Sent: 11 July 2023 07:23
To: tim.rhodes
Subject: Evri *We've been unable to deliver your Parcel



The delivery ‘advance fee’ scam

- OK, so what other clues were there ?
- Evri would not have sent a mail from geraldine.middleton@btconnect.com
- Your ‘who is it from test’ should have moved the s-o-m deal here
- Are you expecting anything from Evri ? If so, check the tracking number from the original mail and match it against the (fake) one given.

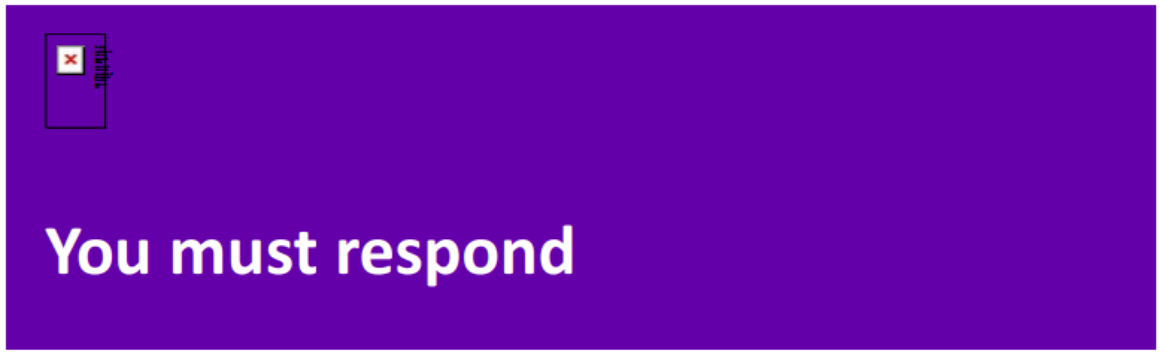
- So we have some new rules
  - Follow these if your s-o-m has moved above zero (here, the ‘from’)
  - Act slowly, have a coffee
  - If a number (tracking, account etc) is quoted, check it

- This mail scam relies on
  - Of the 50,000 sent out, a significant number will have an outstanding Evri delivery (or you might make the assumption above)
  - Either way, there is FOMO “fear of missing out” / a loss (BIG flag)
  - You will act hastily
  - You will make assumptions, even after the flag

The service threat scam (page 1)

From: Communications <btcomms@btanalysis.com>
Sent: 28 September 2023 08:50
To: tim.rhodes@btinternet.com
Subject: ! You must respond now

Here's all you need to know about your order

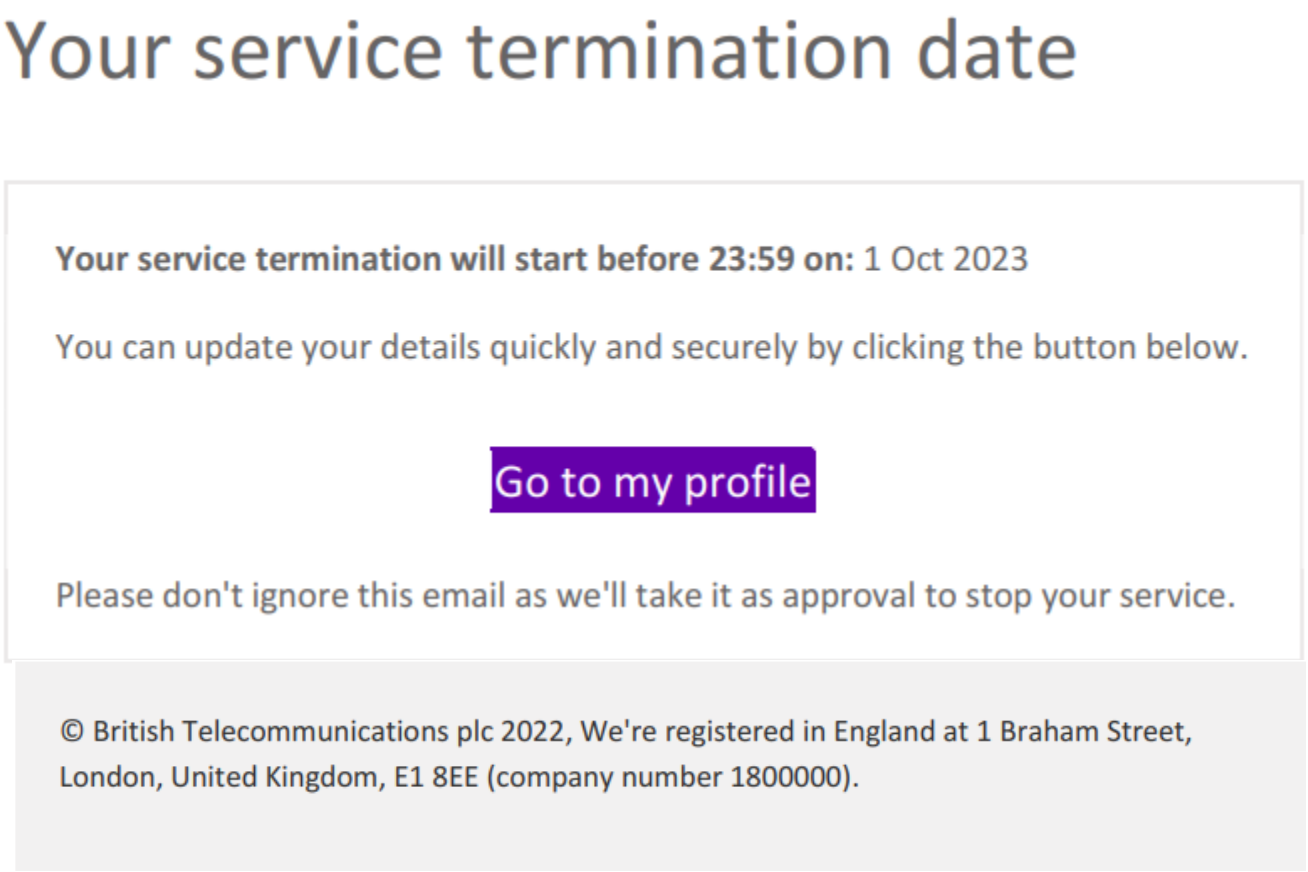


BT ID: t*m*r*o*e*@btinternet.com

We've had no response from you as of yet, so we're reaching out to you once again

You must update your profile details now, otherwise we'll proceed with the planned service termination

The service threat scam (page 2)



Your service termination date

Your service termination will start before 23:59 on: 1 Oct 2023

You can update your details quickly and securely by clicking the button below.

Go to my profile

Please don't ignore this email as we'll take it as approval to stop your service.

© British Telecommunications plc 2022, We're registered in England at 1 Braham Street, London, United Kingdom, E1 8EE (company number 1800000).

The service threat scam

- This mail is often not directly about asking for money – they want your details
- Here, the ‘from’ address almost looks convincing, but it’s not bt.com
- The ‘To’ address is you
- Flag: there is **urgency** (“you must respond now”) (“update details quickly”)
- Flag: It mentions an ‘order’ – have you got one outstanding ?
- Flag: a **threat** “we’ll proceed with the planned service termination”
- Flag: a **threat** – ignore the mail and they will stop the service
- This is a big threat as it hints it involves internet, e-mail etc.

- (The s-o-m should be turning to red about now)

- Ok, time to update the scam-o-meter list !

Running scam-o-meter warning flags list

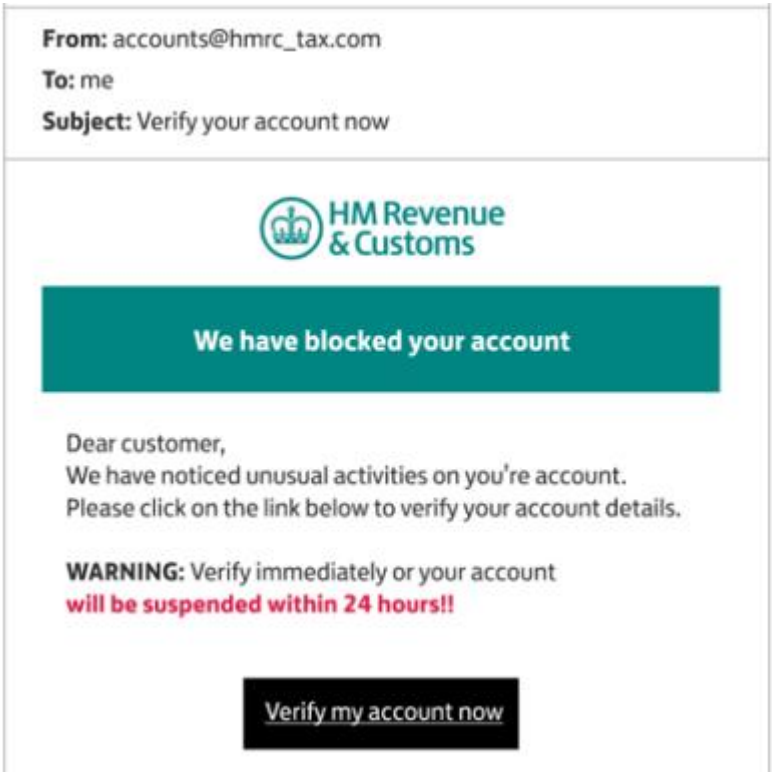
- Unconnected with apparent sender ‘From’ address
- Non-specific ‘To’ address ‘undisclosed-recipients’ / ‘recipients’ / blank
- Promise of **reward** / benefit (‘greed’) or **loss** / penalty (‘fear’)
- Unconnected with apparent sender mail reply address (+2 pips for gmail)
- Sniff test ! You are being offered something for nothing / too good to be true
- You are being asked to act **urgently** or else
- There is a **threat**
- The threat is significant disruption rather than money

- *React slowly*
- *Apply common sense*

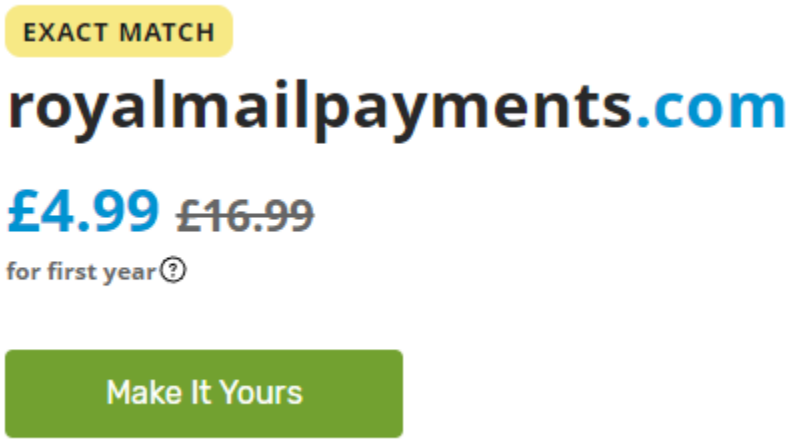
- Ok, now for a few quickies to illustrate other types to watch for

Quickies

- Urgent action or loss



So easy …



Quickies

- TV Licence

From: MyLicense ~ TV <noreplay.tv.subscription@leicesterarena.co.uk>
Sent: Friday, September 29, 2023 3:07 PM
To: tim.rhodes@btinternet.com
Subject: Subscription

TV LICENSING

Renew your TV Licence

Reference: TV36856
Email: tim.rhodes@btinternet.com

The DIRECT DEBIT for your TV license Number 74238236856 From your account had been cancelled, This means we won't be able to take your next payment.

To remain licensed, Please set up a new DIRECT DEBIT. It's quick and easy to do online. Please take care of this straight away or we may have to revoke your license.

Get Started ↣

You are licensed until [29/09/2023 - 16:07:01].

Quickies (test here !)

- You have been selected

You have been selected for an Oral-B iO 9 series! <xboxreps@engage.xbox.com>

To tim.rhodes@btinternet.com

If there are problems with how this message is displayed, click here to view it in a web browser.

YOU ARE OUR WINNER!

Reward: Oral-B iO Series 9 offered by Boots!

A delivery fee may apply

Your unique code:

#UK01-24142

Click here to get the reward

Quickies

- “You have been selected”

From: You have been selected for an Oral-B iO 9 series! <xboxreps@engage.xbox.com>
Sent: Tuesday, August 29, 2023 3:59 PM
To: tim.rhodes@btinternet.com
Subject:

YOU ARE OUR WINNER!

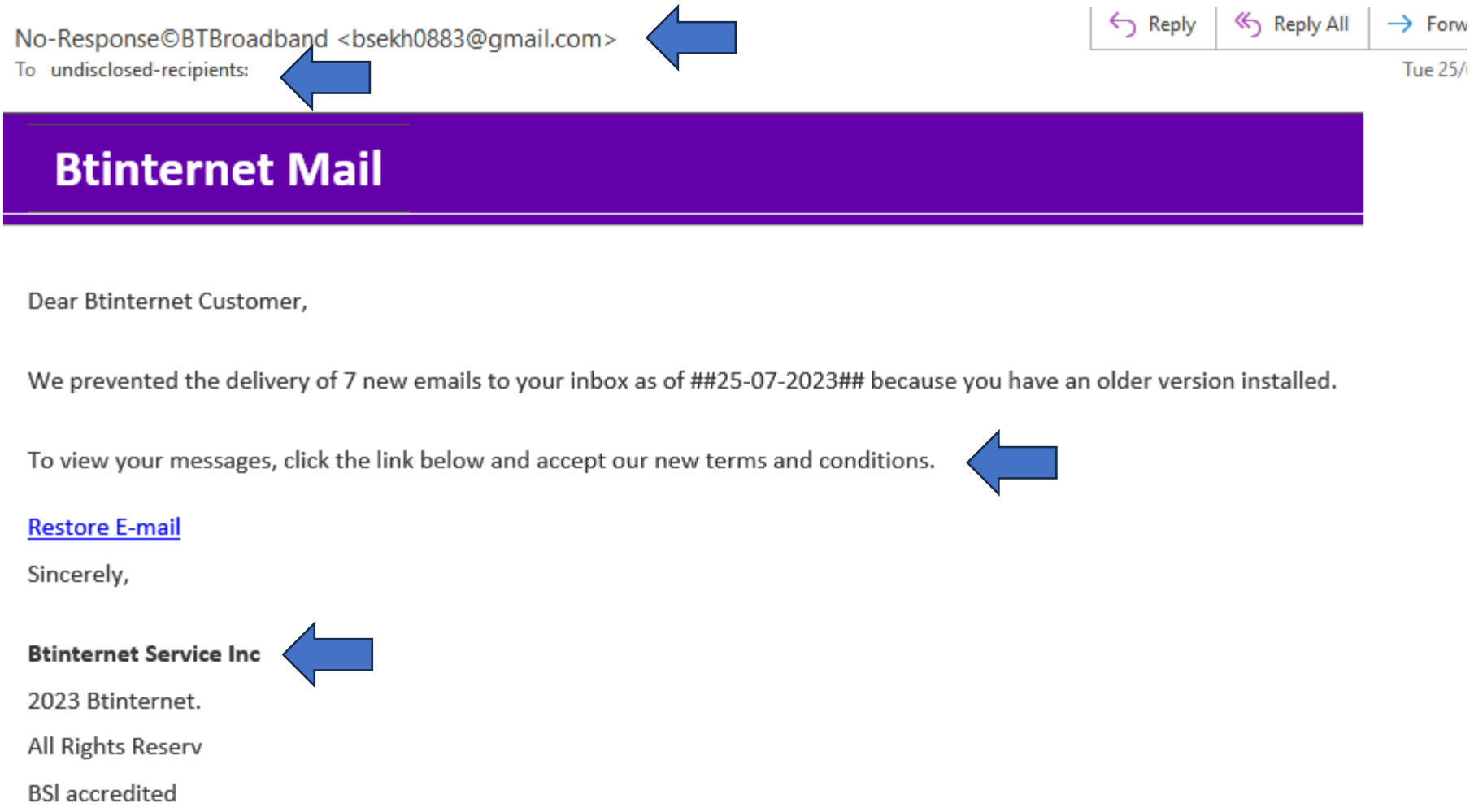
Reward: Oral-B iO Series 9 offered by Boots!

A delivery fee may apply
Your unique code:

#UK01-24142

Click here to get the reward

More examples – 20 seconds each for you to recognise trap



No-Response©BTBroadband <bsekh0883@gmail.com>

To undisclosed-recipients:

Reply | Reply All | Forw

Tue 25/

Btinternet Mail

Dear Btinternet Customer,

We prevented the delivery of 7 new emails to your inbox as of ##25-07-2023## because you have an older version installed.

To view your messages, click the link below and accept our new terms and conditions.

Restore E-mail

Sincerely,

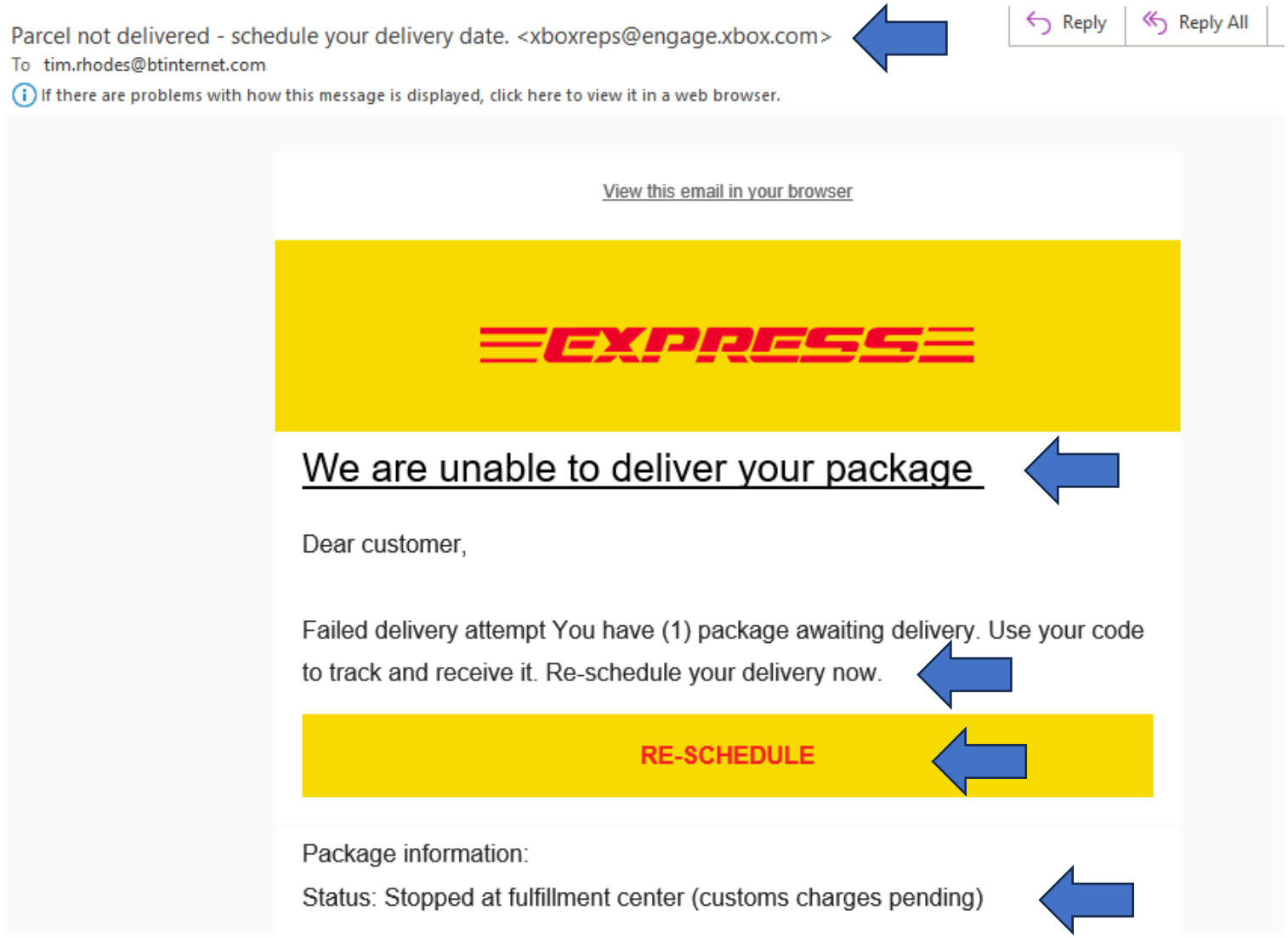
Btinternet Service Inc

2023 Btinternet.

All Rights Reserv

BSI accredited

More examples – 20 seconds each for you to recognise trap



More examples – 20 seconds each for you to recognise trap

Congratulations! Complete the short survey and get J'adore by Dior!

Consumer survey <contact@news.boots.co.uk>

To tim.rhodes@btinternet.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Reply | Reply All | Forwar

Thu 17/08/

Reward: Dior J'Adore offered by Boots.

A delivery fee may apply

Your unique code:

#UK01-86702

Click here to get the reward

More examples – 20 seconds each for you to recognise trap

Western Union/MoneyGram Money Transfer Scam Victims

Christopher A.Wray <test@test.net>
To Recipients

Reply | Reply All | Forward | ...
Sun 03/09/2023 01:23

FBI Headquarters
935 Pennsylvania Avenue, NW
Washington, DC 20535 USA

Attn: Beneficiary

After proper and several investigations by the Western Union, Money Gram, International Monetary Fund (IMF) and United Nations (UN) Offices we found your name amongst those that have sent money through Western Union, Cash App, Zelle, Venmo, Bank Transfer/Deposit and Money Gram in the course of receiving your Inheritance, Lottery, United Nation compensation funds which proves that you have truly been swindled by those unscrupulous persons by sending money to them through the above mentioned means.

To this regard United Nations (UN) held a meeting with the Board of Directors of WESTERN UNION, MONEYGRAM, INTERNATIONAL MONETARY FUND (IMF) the FBI alongside with the MINISTRY of FINANCE. As a result of our investigations it was agreed that the sum of Six Million Five Hundred Thousand United States Dollars (U.S. $6, 500,000.00) should be transferred to you from the funds set aside by The United States Department of the Treasury to compensate scam victims.

Stupid filter

The compensation scheme is open to people who wired money to scammers via Western Union and Money Gram between January 1, 2004 to December 19, 2021, the deadline for lodging these claims is December 30, 2023.

This case is being handled and supervised by the FBI therefore we have submitted your details to affect the transfer of your funds to you. Contact the Western Union agent office through the information below:

Contact Person: Betsy Holden
Address: Western Union Post Office, California
Email: betsyholden940@gmail.com

Yours sincerely,
Christopher Wray

Now, a ‘non-scam’ scam

··King Charles III Coronation Coin FREE for you!··

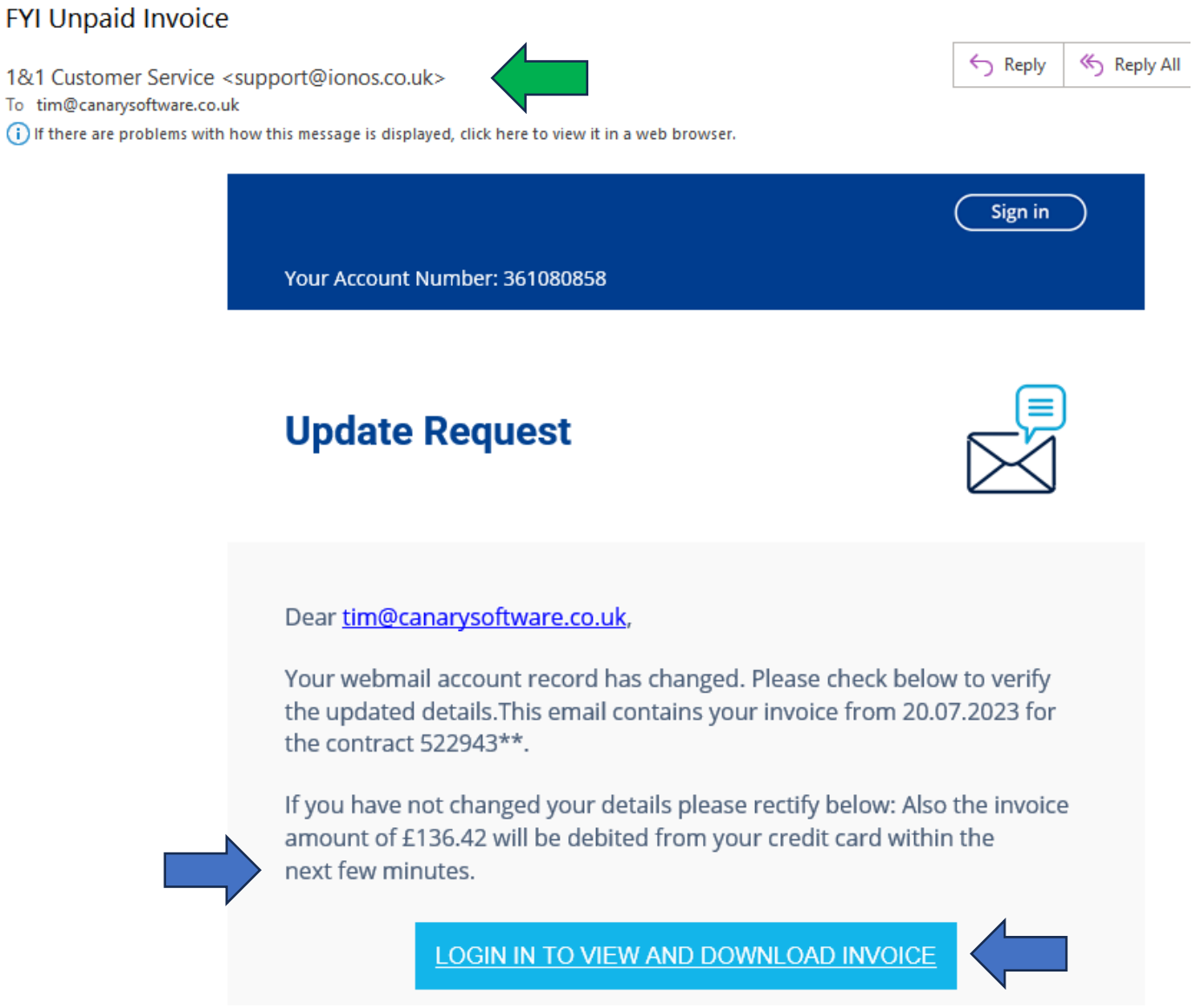
Â·Â·Â·London Mint Office with Your Reward <info@news.excellent-email.net>
To tim.rhodes@btinternet.com

Reply | Reply All | →

If you are having difficulties reading this email correctly click here

JUST RELEASED: King Charles III Coronation Coin

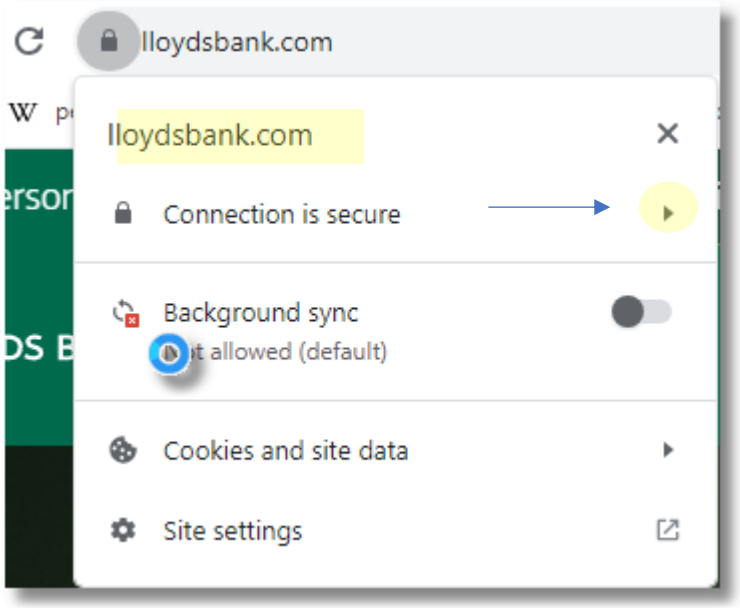
… and finally, a (half) ‘professional’ one



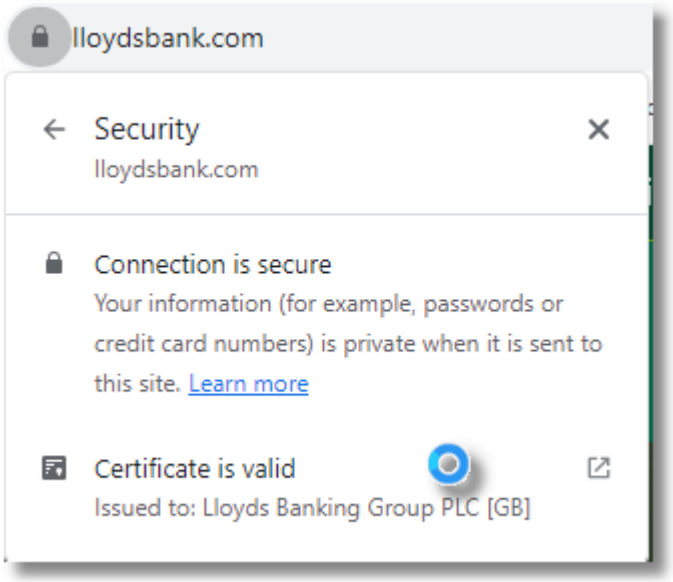
Tip : Check any web site you make payments on

E.G Lloyds Bank

Click on the ‘lock’ icon

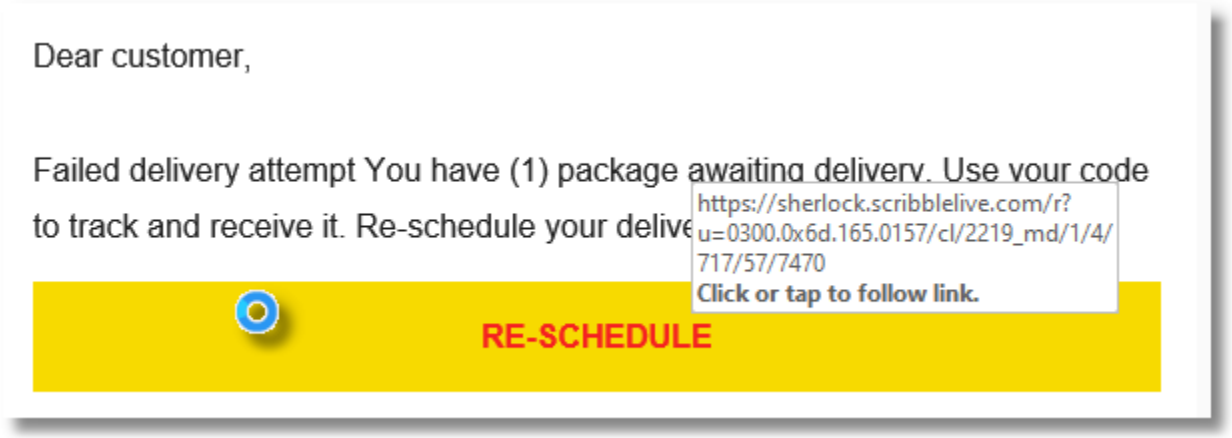


This confirms the connection is secure



For the paranoid: click on the mini arrow for full details

Tip : hover the mouse / finger over a link to see where it's going

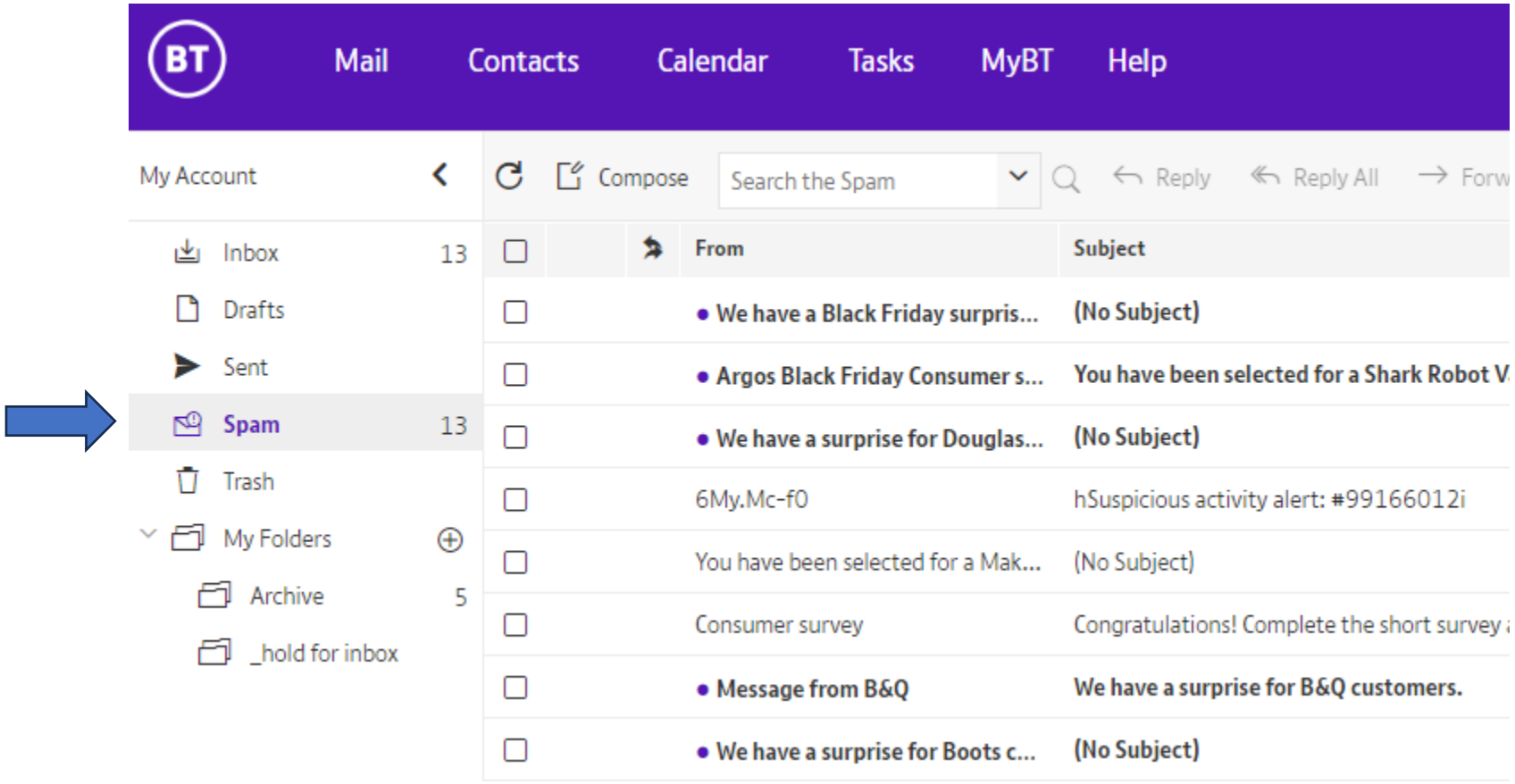


Supposedly from UPS Express …

But hovering shows you will be taken to sherlock.scribblelive …

Obviously not UPS !!

Tip : Your e-mail provider will have anti- spam tools



In conclusion…

- Primary rule – don't react to any mail with a threat or "too good to be true"
- You know the signs
  - odd sender, not matching the organisation it purports to be
  - Seemingly for you personally, but sent to 'undisclosed recipients' etc
  - mails conveying a sense of urgency generally
  - there is a threat to cease service or require payment
  - there is a threat of a security breach
  - there is mention of an advance payment (e.g. delivery fee)
  - mails with an attractive purchase offer or other promise of money
  - anything to do with investments / pension opportunities
- For any of the above, never click a link or download a file !

- *I hope the session has been worthwhile and given you more confidence to recognise fraudulent mails*