

# Email Scams



ComputerPals  
HOW2  
PROCEDURES

## How to spot an email scam ...

If it is too good to be true ... IT'S A SCAM!  
If the world is about to collapse ... IT'S A SCAM!

- When you receive an unexpected email, or even if it just coincidentally arrives when you do stuff, **be warned.**

All of the examples here are REAL email scams and have one thing in common: They are designed to solicit a response.

- Take your time**, the refund from the Tax office or your disconnection from Netflix can wait. If either looked true then simply contact them by email or telephone, using an address or number **YOU** have independently looked up (not the one the message provided).

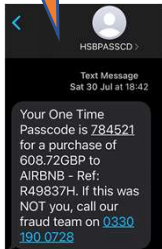
**UNDER NO CIRCUMSTANCES CLICK ON ANY LINK PROVIDED**

- By doing this you may be fooled in seeing a 'spoof' login screen asking you to enter further details ...
- If you continue you may become subject to other scams, like being phoned (from your Bank) about the original scam, etc.

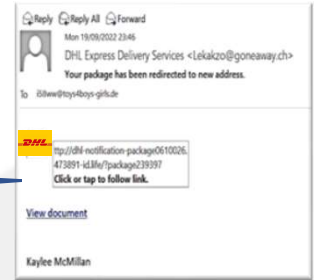
**Be warned as in this case they already know a lot about you!**

**ALSO:** Text messages (and social media) may also be scams, like this one below asking you to ring HSBC

Strange Purchase



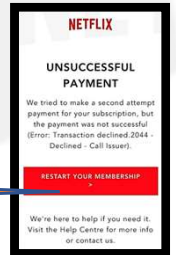
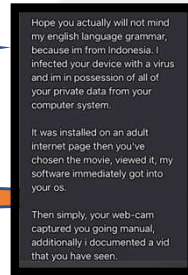
Package Redirection



Weird demand for money



Sexual Treat



Pending Disconnection



Monetary Refund 😊

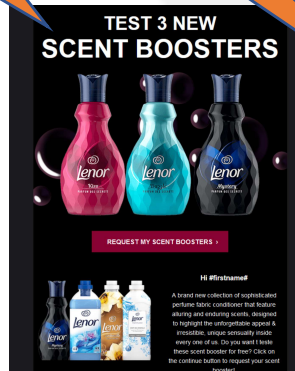
Tax Back 😊



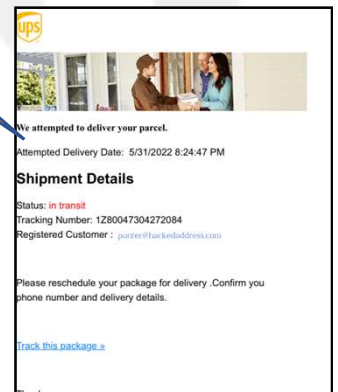
Expired Contracts



Free Goods



Failed Delivery

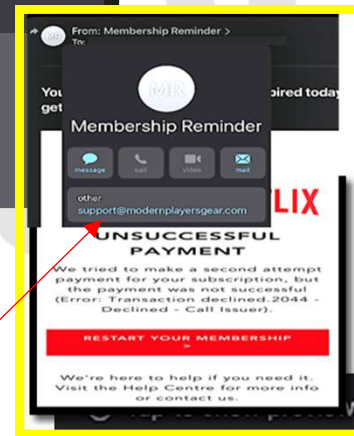
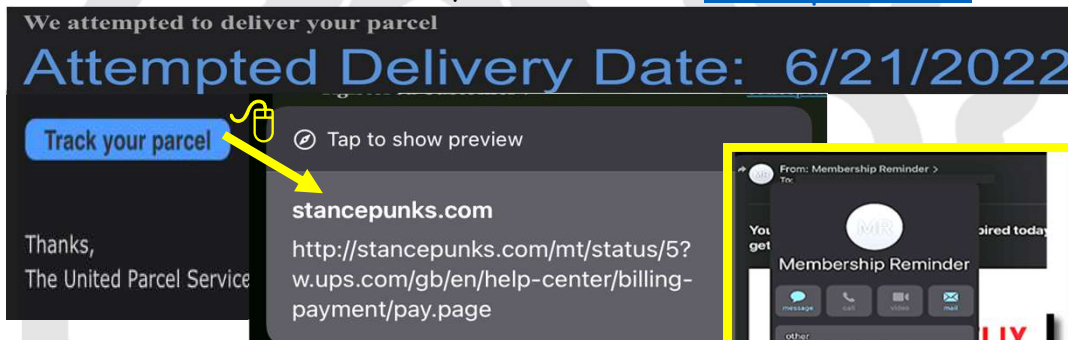
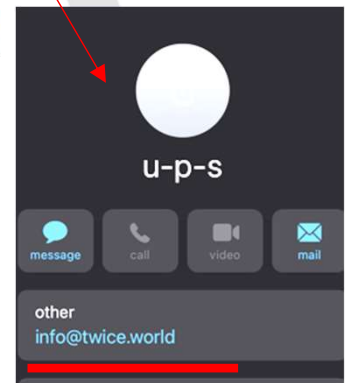
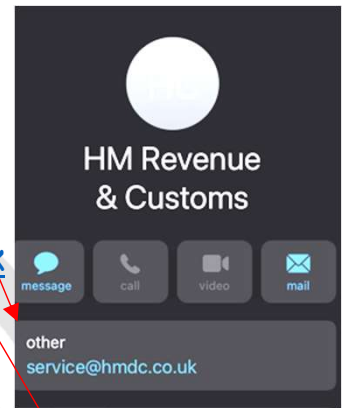


## How to spot an email scam ...

### HOW TO (try to) SPOT A SCAM!

When you receive an unexpected email, click on the sender name to see who sent it, DOES IT MATCH the companies Domain\*

- HM Revenue and Customs email was sent from [service@hmcd.co.uk](mailto:service@hmcd.co.uk)
- Example 1: UPS message arrived from [info@twice.world](mailto:info@twice.world) not UPS
- Look at the link, (be careful) long click and hold over the link, read the details. Not from UPS?, the domain is [stancepunks.com](http://stancepunks.com) ???



- Example 2: The Netflix Scam ...
  1. Who sent it?  
By clicking on the sender we get [support@modernplayersgear.com](mailto:support@modernplayersgear.com) ??
  2. Inspecting the link, LONG CLICK and HOLD, not Netflix but [com-appslnon.com](https://com-appslnon.com) (NB: read from the right dot by dot back from .COM)
  3. Look up the owner of this domain name by using the [who.is](http://who.is) lookup service.
  4. This lists the owner, but look at the date the site was created and the date the email was sent !! **Alarm Bells!**

Re: New Activity other device, at Mon, July 18, 2022 9:16 AM  
 NB: Scammers can hijack real websites, so not a guarantee

### Other Check Tools

- DNS Lookup: [who.is](http://who.is)
- Phishtank: <https://phishtank.org>
- Web of Trust: <https://www.mywot.com>
- Scan URL: <https://scanurl.net>
- DNS lookup: <https://dnschecker.org>

### How to Report

Send to [report@phishing.gov.uk](mailto:report@phishing.gov.uk)  
 Send text messages send to 7726  
 (SPAM using phone keypad)

Also see: [computerpals.co.uk/furtledox.pdf](http://computerpals.co.uk/furtledox.pdf)

### \* The Technical bit.

The DOMAIN NAME: Every web/email address has a domain associated with it. In an email the domain name is directly after the @ sign, and after HTTP:// in a web address. These names are separated by dots., ie: [www.gov.uk/tax-codes](http://www.gov.uk/tax-codes) and before any /'s. Read them right to left, so UK then GOV, then WWW. The domain name is very difficult to spoof, but easy to make confusing. So none of the following are real. Watch for other dots, ? or hyphens [www.gov-tax.uk](http://www.gov-tax.uk), [www.reclaim-your-tax.gov.uk](http://www.reclaim-your-tax.gov.uk), [www.money-back.gov.uk.hrmc.uk](http://www.money-back.gov.uk.hrmc.uk), [hrmc.uk.moneyback@taxoffice-refunds.com](mailto:hrmc.uk.moneyback@taxoffice-refunds.com) and [xyz.com/index.php?gov.uk](http://xyz.com/index.php?gov.uk) **click with care!**

