



# Identifying malicious emails



## Introduction

Unfortunately, the Covid-19 has increased the number malicious emails being sent. The HFMA's IT team has produced eight red flags that help identify them – as more NHS staff are working from home, and doing unfamiliar jobs, this reminder might be useful.

### Red flag 1: the sender's email address is strangely formatted

Always be cautious of emails from people you have not contacted before or are not familiar with - particular care should be taken with odd domain names, such as:

**John.smith@voip.0365messagescenter.com**

Checking the domain name is the single most important action that you can take and should pick up a good percentage of malicious emails.

### Red flag 2: it is not addressed to you personally

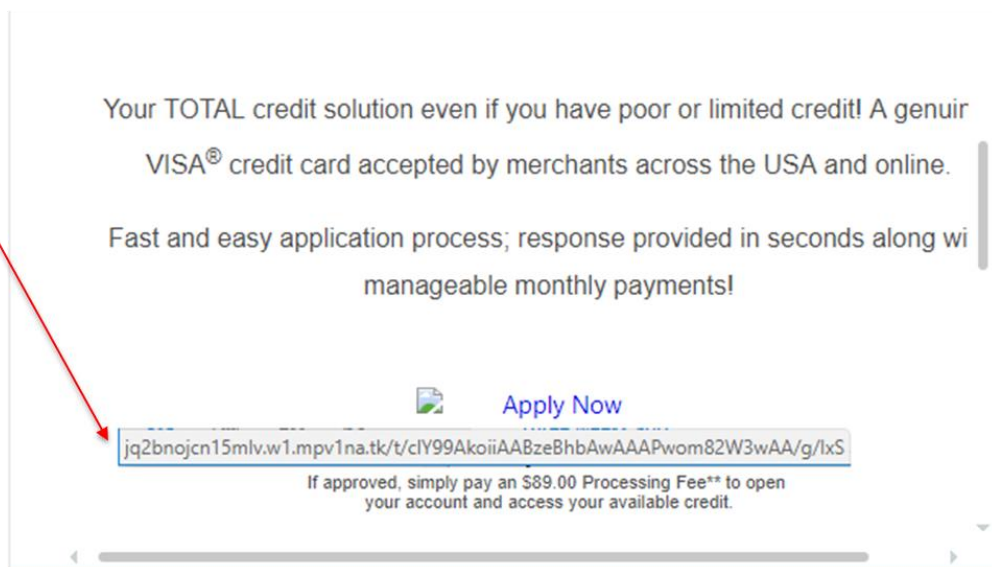
An email that is not addressed to you or uses a common salutation may be suspicious. It will not always be the case, but it is worth taking into consideration:



### Red flag 3: the URL embedded in the email is strange

Hover over any of the URLs embedded in the email with your mouse to check whether the URL looks reasonable:

The email explicitly states that it is from a credit provider that utilises the renowned VISA services, however, the URL embedded that is shown when hovering over 'Apply Now' looks odd and does not indicate a safe URL



### Red flag 4: the email has attachments

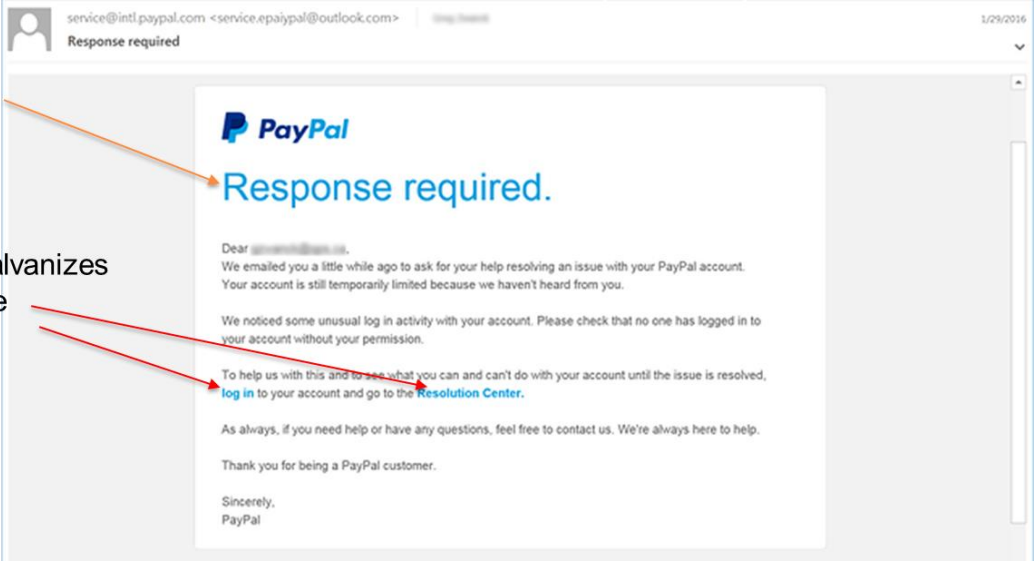
Always be wary of any attachment, especially from unfamiliar email addresses. It may be fine but proceed with caution.

### Red flag 5: the email asks you to do something

Many malicious emails are a 'call for action', for example, they include a button that states 'click; here' or the email conveys a sense of urgency such as 'late payment' or 'outstanding balance'.

Call for action

Call for action galvanizes you to click these malicious URLs



### Red flag 6: the content looks odd

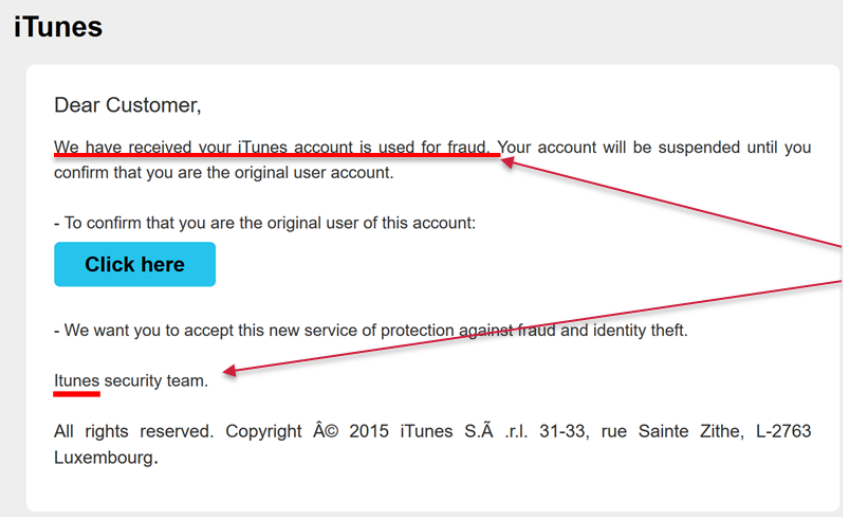
The content of the email is unfamiliar and does not relate to yourself or your job role.

### Red flag 7: the language, spelling and grammar contains errors

The email looks as if an online translation service has been used to translate it into English. An example is set out below.

★ **Apple support** <Apple@web4.profiwh.com>  
 from: Apple support <Apple@web4.profiwh.com>  
 date: Tue, 23 Feb 2016 10:37:55 +0100 (CET)  
 subject: Apple & iCloud Service New Notice

Note the unusual email address (see tip 1)



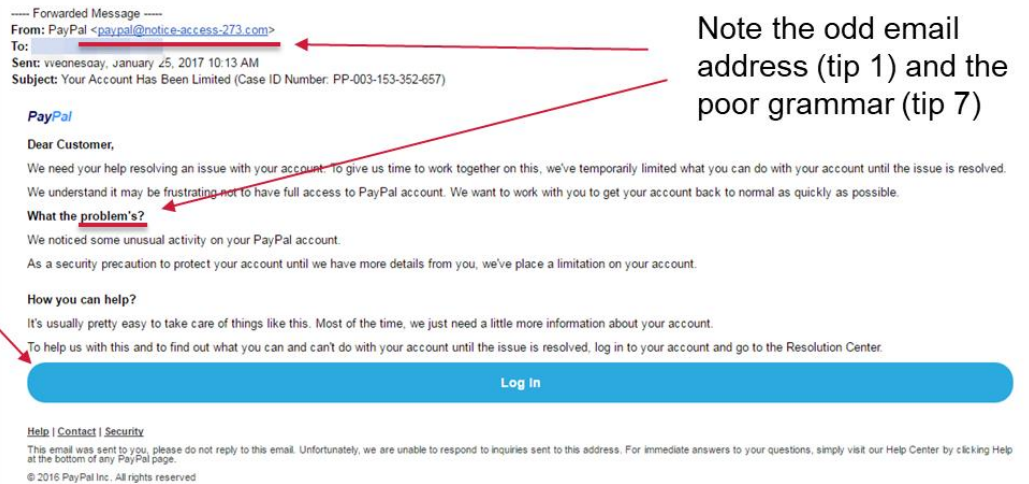
As well as the odd grammar and formatting

## Red flag 8: the email is phishing for information

Be wary of emails asking for personal information, organisation details or banking information. It may seem innocuous, but the information could be used to impersonate you.

The request for information may not be in the email itself, but it may link to another site such as a fake PayPal, Office 365 or NHS sign-in page so it is important to apply the other tests to identify this as a malicious email. If in doubt, login to your account through the website than via a button or link in an email:

This button would take you to a fake PayPal login page that would subsequently steal your login details



Note the odd email address (tip 1) and the poor grammar (tip 7)

## Further guidance

Any fraudulent emails should be reported to the [NHS Counter Fraud Authority](#) and your local counter fraud team. [GOV.UK](#) has also issued advice on how to avoid and report internet scams and phishing.

Similar guidance is available from:

- [Action Fraud UK](#)
- [ACCA](#)
- [The National Cyber Security Centre](#)
- [BBC](#)

## About the HFMA

The Healthcare Financial Management Association (HFMA) is the professional body for finance staff in healthcare. For nearly 70 years, it has provided independent and objective advice to its members and the wider healthcare community. It is a charitable organisation that promotes best practice and innovation in financial management and governance across the UK health economy through its local and national networks.

The association also analyses and responds to national policy and aims to exert influence in shaping the wider healthcare agenda. It has particular interest in promoting the highest professional standards in financial management and governance and is keen to work with other organisations to promote approaches that really are 'fit for purpose' and effective.

The HFMA offers a range of qualifications in healthcare business and finance at undergraduate and postgraduate level and can provide a route to an MBA in healthcare finance. The qualifications are delivered through HFMA's Academy which was launched in 2017 and has already established strong learner and alumni networks.

© Healthcare Financial Management Association 2020. All rights reserved.

While every care had been taken in the preparation of this briefing, the HFMA cannot in any circumstances accept responsibility for errors or omissions, and is not responsible for any loss occasioned to any person or organisation acting or refraining from action as a result of any material in it.

### HFMA

1 Temple Way, Bristol BS2 0BU

T 0117 929 4789

E [info@hfma.org.uk](mailto:info@hfma.org.uk)

Healthcare Financial Management Association (HFMA) is a registered charity in England and Wales, no 1114463 and Scotland, no SCO41994.

HFMA is also a limited company registered in England and Wales, no 5787972. Registered office: 110 Rochester Row, Victoria, London SW1P 1JP

[www.hfma.org.uk](http://www.hfma.org.uk)