

How to identify phishing emails

Article Number: 219 | Rating: Unrated | Last Updated: Fri, Nov 23, 2018 at 4:26 PM

Please be aware we have seen an increase in phishing attempts in the recent few weeks with emails being faked coming from Microsoft.

As you can see in the below image it seems to be from an office.com email address, however there is two ways you can tell if its fake.

Mon 29/10/2018 14:34

Microsoft Business Team <MicrosoftBusinessTeam329e71ec88ae4615bbc36ab6ce41109e@office.com>

Re: Your Office Business Essentials Invoice is ready

To Adam Reynolds

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Your Office Business Essentials Invoice is ready

To pay your invoice:

[Sign in to the customer Portal](#)

Note: If you are paying by credit card or direct debit, your payment method will be charged within one day of the invoice date.

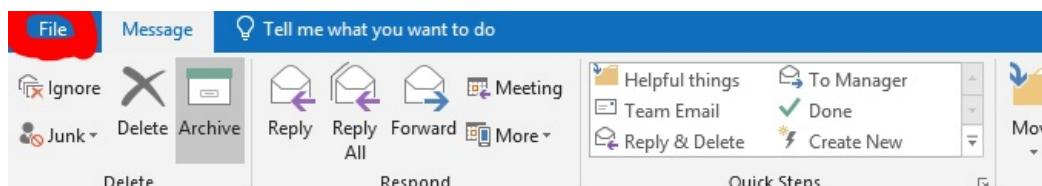
[Click here for instructions on how to read the PDF with NVDA and to ensure a quality user experience.](#)

Thank you,
The Microsoft Online Services Team

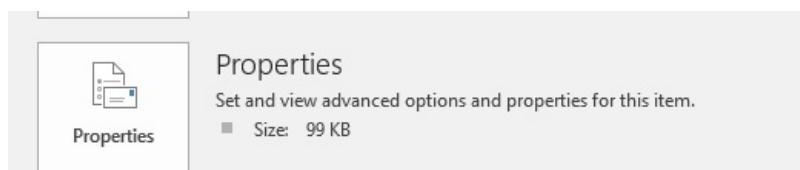
This email originated from OUTSIDE the Internet Central Corporate Network. Please treat HYPERLINKS and ATTACHMENTS with caution.

1. Checking the headers of the email

If you have the email open, you can see at the top left you have "file"



Once in file, go to "properties"



Once in here, if you scroll down you will see a senders domain, in this case the sender is not Microsoft.

```
header.d=none;jc.co.uk; dmarc=none action=none header.from=;
Received-SPF: Fail (protection.outlook.com: domain of davidbrown.com
does not
designate 88.99.21.183 as permitted sender)
```

2. The second way of checking is by hovering over (ensuring not to click) the link in the email

You
is re
To pay y
Click or tap to follow link.

http://tesslamacraft.co.uk/azolharqzp/zrx36rxnhwzqra/?target=-7ebrqcgqaaaomiamegwaf0w8yvsreqorcqorduirdvoax9hzgnvbwjv_2nlowu2nta3aanjnq&al=23003&ap=-1&subacc=anna29.10.01&subacc2=20181029ae83f47bid107330&esub=-7ebrqcgqp7uc7qwomiamegwpigjpbwfybaq8aag8-5dzberekeqkieq1ceq1ab25smgaaf2fk29ty29tm_mwzknmflmzyaazhj

E:

[Sign in to the customer Portal](#)

Once again, I hovered over the link and you can certainly see that this is not a legitimate website.

Posted by: Keira Tait - Fri, Nov 23, 2018 at 4:26 PM. This article has been viewed 3617 times.

Online URL: <https://kb.ic.uk/article/how-to-identify-phishing-emails-219.html> (<https://kb.ic.uk/article/how-to-identify-phishing-emails-219.html>)