E-mail spam guide

It’s important to avoid getting malign items onto your PC, and one way for them to enter is via e-mail. Nasty e-mails normally pretend to be from a person or (more frequently) an organisation that you know and will seek to masquerade as the real thing.

They often contain ‘malware’ that may compromise / damage your machine, steal passwords, or hold you to ransom by encrypting your data.

There are a few simple rules which you can follow which will catch a good percentage of bad mails created by ‘amateur’ crooks.

Whatever, you need to ensure that McAfee and Malwarebytes are up to date and running.

E-mails can contain links of attachments which (bad case) load software on your machine to ‘log’ your key presses and send them to the spammer. These include the usernames and passwords you use to connect to (e.g.) banks etc. They could take over your e-mail account, lock you out and and use that for nefarious purposes.

E-mail spam guide

A scam message will generally have the following characteristics

- There is a time pressure to reply quickly
- There is a threat of account closure or money loss if you don’t do so

- The sender was blank / ‘recipients’ / ‘me’

- It seemed to be (say) B T, but the mail had an address like dogfur@jahst.ru

- ***There is a link you have to click or a document to download***

E-mail spam guide – ‘extensions’

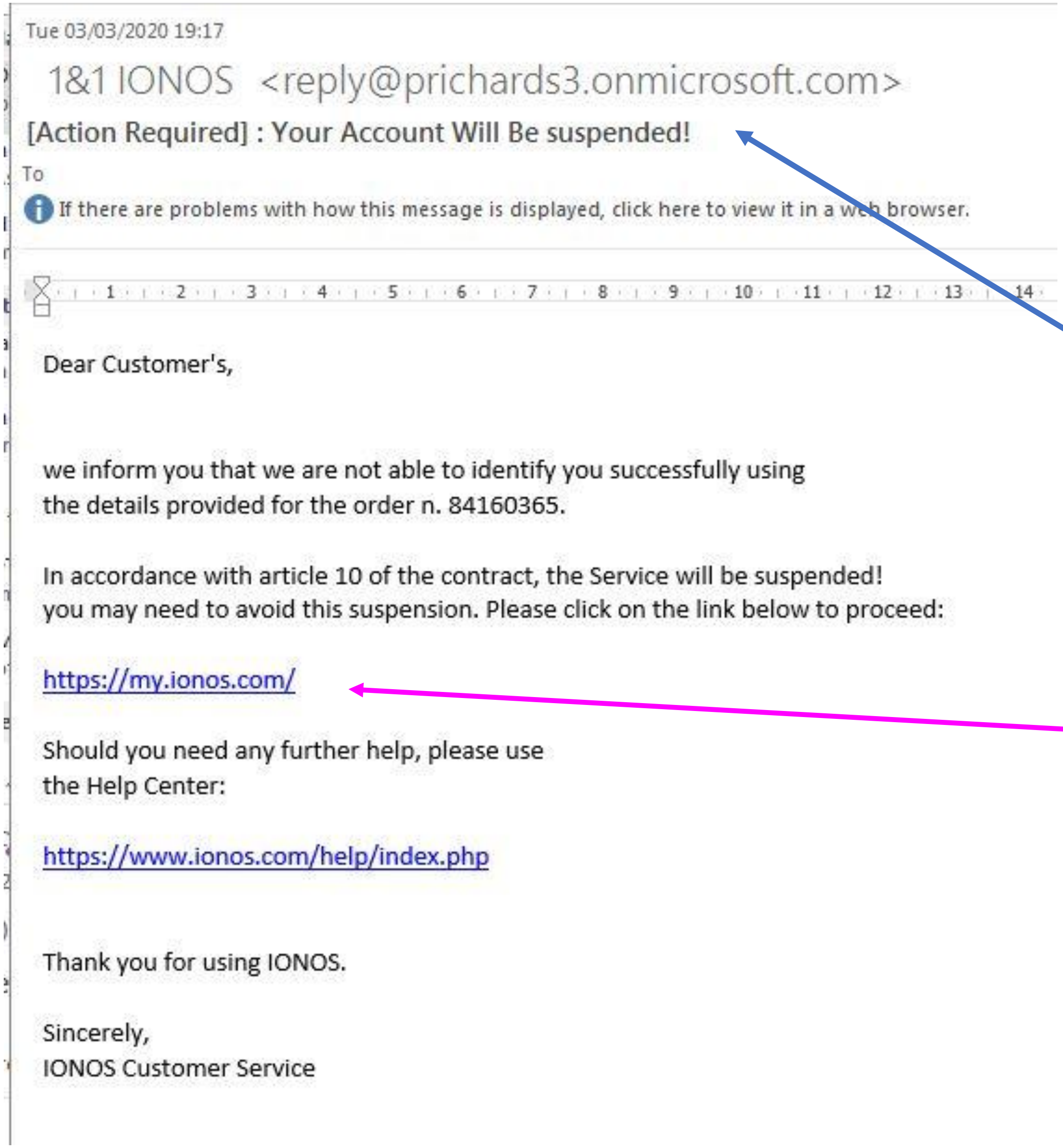
An attachment to an e-mail will have a ‘file name’ e.g. “killik report.pdf”

One crucial element in spam spotting is the extension, which is the bit after the last dot – in this case “.pdf” . Last dot, because if you have “virus.doc.exe” what matters is the “.exe”. The spammer puts “.doc” to make you think it may be ok.

Some rules on file names are

- “.pdf” (for documents) is generally safe from known senders (and why open it if you don’t know the sender or were expecting something)
- “.jpg” (for pictures) is generally safe from a personally known source
- “.doc” of “.docx” (a word document) is generally safe from a known source, but they can still carry ‘malware’, so exercise caution. Never open something the sender says “I’m forwarding this to you…” – only open things they originated
- “.exe” / “.iso” / “.msi” / “.cpl” should **NEVER be opened** unless you are really sure and confident that it is from a completely trusted source and you have ether ordered it or had a dialogue with the sender.

E-mail spam guide



Tue 03/03/2020 19:17

1&1 IONOS <reply@prichards3.onmicrosoft.com>

[Action Required] : Your Account Will Be suspended!

To

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

Dear Customer's,

we inform you that we are not able to identify you successfully using the details provided for the order n. 84160365.

In accordance with article 10 of the contract, the Service will be suspended!
you may need to avoid this suspension. Please click on the link below to proceed:

https://my.ionos.com/

Should you need any further help, please use the Help Center:

https://www.ionos.com/help/index.php

Thank you for using IONOS.

Sincerely,
IONOS Customer Service

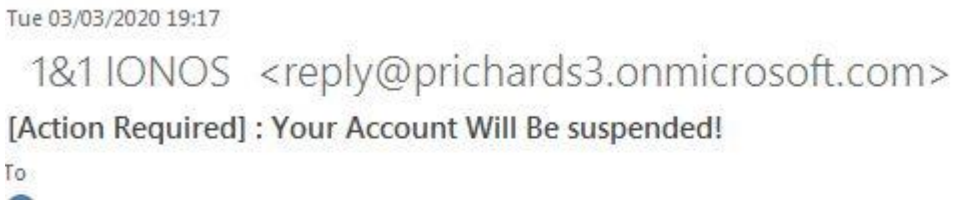
In this example, the mail purports to be from Ionos, our mail provider.

There is a threat – "do something or you will be cut off". That's a spam hint, unless you know that you haven't paid the bill

There is then an attachment to download, or a link to follow to a web site. Here it's a link to http:/my.ionos.com

Let's look more carefully

E-mail spam guide



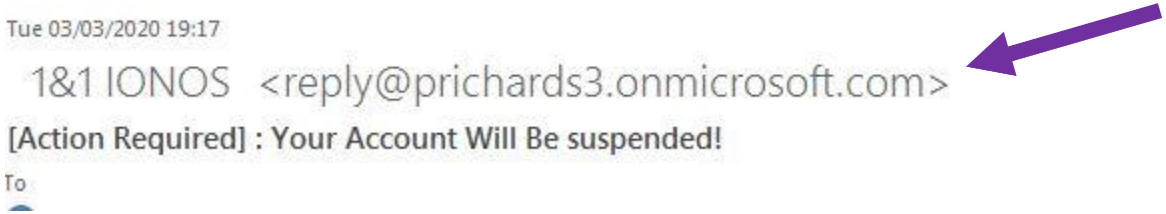
Tue 03/03/2020 19:17

1&1 IONOS <reply@prichards3.onmicrosoft.com>

[Action Required] : Your Account Will Be suspended!

To

The clue from this amateur attempt is immediate – have you spotted it ?



Tue 03/03/2020 19:17

1&1 IONOS <reply@prichards3.onmicrosoft.com>

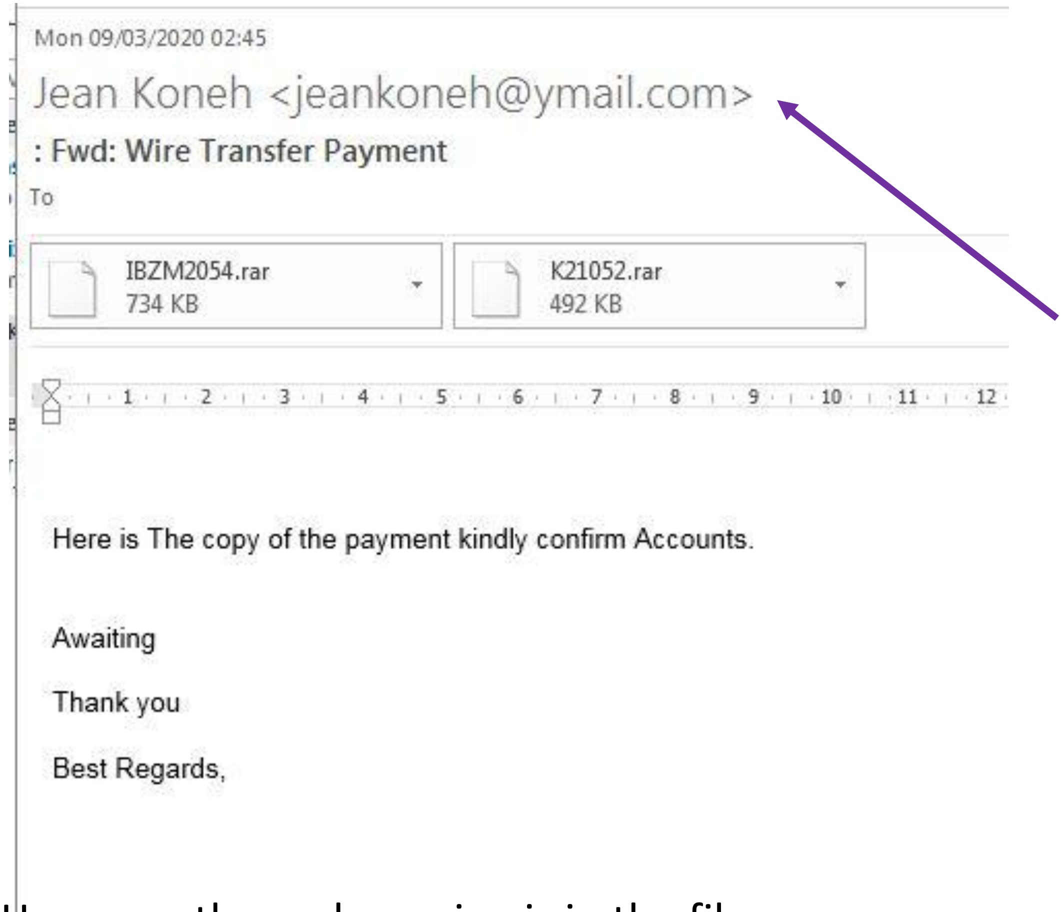
[Action Required] : Your Account Will Be suspended!

To

It’s much harder (though still possible) for a bedroom hacker to spoof the ‘from’ address. You can be pretty sure that Ionos do not send out legal account terminating mails from “prichards2.onmicrosoft.com” – it’s spam

Do not press and link, but do press “delete”.

E-mail spam guide



Mon 09/03/2020 02:45

Jean Koneh <jeankoneh@ymail.com>

: Fwd: Wire Transfer Payment

To

IBZM2054.rar
734 KB

K21052.rar
492 KB

Here is The copy of the payment kindly confirm Accounts.

Awaiting

Thank you

Best Regards,

This purports to be an invoice for something you have bought. It's obviously false.

First the e-mail has not come from a company, but from some non-descript address

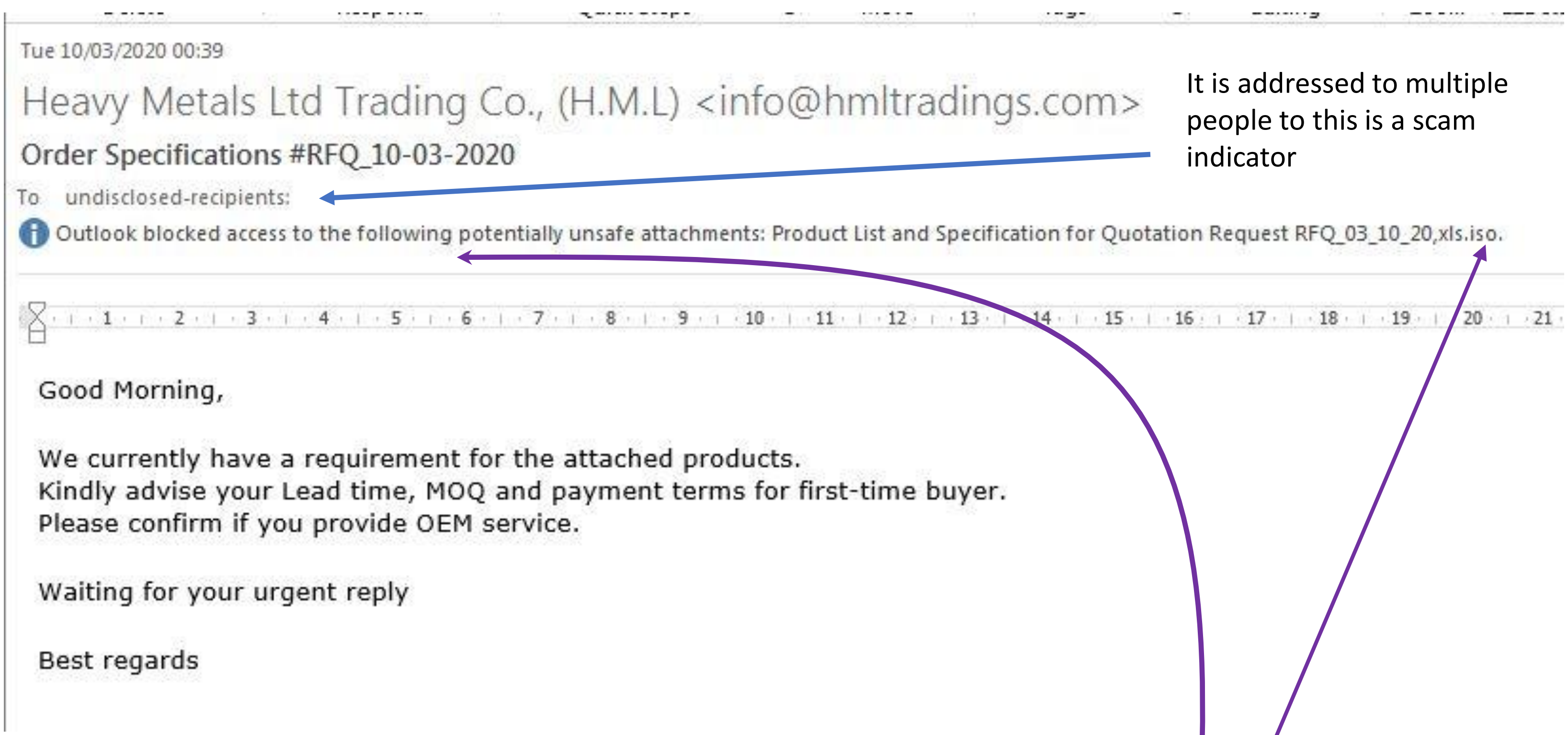
Then, it uses US terminology in the title - 'wire transfer'

There are no corporate contact details, logo, telephone number of anything else indicating a corporate source – pretty amateur.

However, the real warning is in the file 'extension' – bit after the 'dot' - (".rar'") as this sort of file can carry malware. Basically, be suspicious of anything that is not ".pdf".

Instant delete, and fails all tests.

E-mail spam guide



Tue 10/03/2020 00:39

Heavy Metals Ltd Trading Co., (H.M.L) <info@hmltradings.com>

Order Specifications #RFQ_10-03-2020

To undisclosed-recipients:

Outlook blocked access to the following potentially unsafe attachments: Product List and Specification for Quotation Request RFQ_03_10_20,xls.iso.

Good Morning,

We currently have a requirement for the attached products.
Kindly advise your Lead time, MOQ and payment terms for first-time buyer.
Please confirm if you provide OEM service.

Waiting for your urgent reply

Best regards

It is addressed to multiple people to this is a scam indicator

Important clues here, which are easy to spot.

1 Outlook blocked an attachment, which you can see ended in '.iso', which is a no-no along with the extention '.exe'

2 You can't see any connection with you and don't know the sender

3 Signals instant DELETE