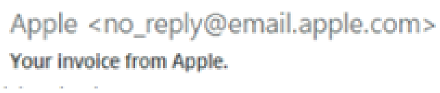
Malicious email guide

ramsac
the secure choice

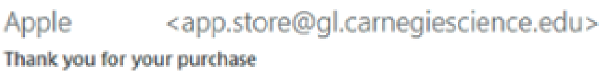
Cybersecurity breaches are the number one threat in today's business landscape. Cyberattacks come in many forms, but one of the most popular is malicious emails, also known as phishing or whaling. Spotting a malicious email is an important skill to master because phishing accounts for 90% of data breaches. And once hit, 15% of people successfully phished will be targeted at least once more in a year. We have created this guide to help you identify malicious emails when you receive them.

Malicious emails often come from odd addresses

The address the email came from will often look suspicious/irregular. This isn't always the case, but many malicious emails will have an unusual 'From' address. The 'From' address can be found at the top of any email chain and usually next to the sender's name.



Apple <no_reply@email.apple.com>
Your invoice from Apple.



Apple <app.store@gl.carnegiescience.edu>
Thank you for your purchase

UNKNOWN
ODD ADDRESS

Ask yourself:

'Do I recognise this 'From' address?'

'Does the address look legitimate?'

'Have I received an email like this before? Could it be compared to a known legitimate message?'

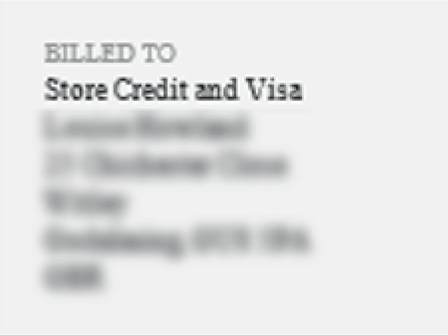
Malicious emails can be bulk sent

Malicious emails are often sent in bulk, meaning you've most likely received one of the thousands of emails that have been sent out to compromise as many accounts as possible. This will mean that the email will have very little personal information. It may include your name and email address, but nothing more. Below is a comparison between a legitimate email with name and address but nothing more.

Ask yourself:

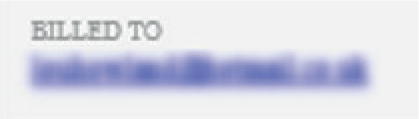
'Could this email have been sent to several other users?'

'Is the content generic?'



BILLED TO
Store Credit and Visa
[illegible]

Full address details



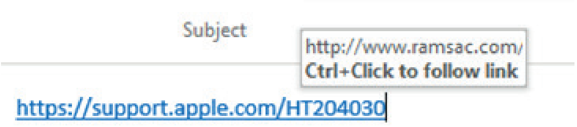
BILLED TO
[illegible]

Just email address

Malicious emails often have hyperlinks

The easiest way to compromise an account is to get the users credentials (username and password). Most attacking emails will ask the recipient to click on a link and type in these details.

The links themselves may appear legitimate, but if you hover over them with the mouse a different address will likely appear (see below):



Subject
http://www.ramsac.com/
Ctrl+Click to follow link
https://support.apple.com/HT204030

Ask yourself:

'Is the email asking me to go to a hyperlink?'

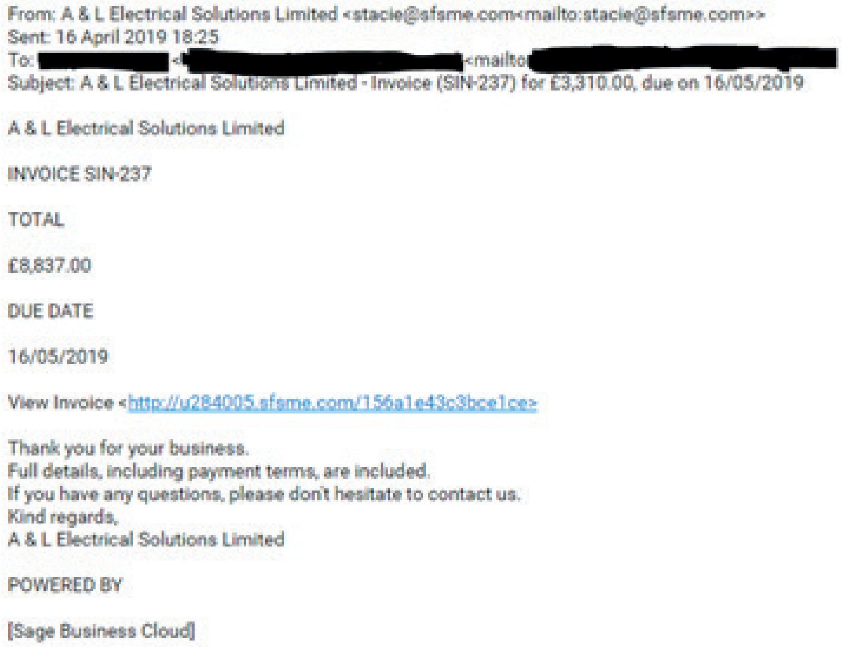
'Does the hyperlink point to the correctly displayed location?'

If in doubt don't click a link unless you are certain it is safe.

Malicious email content

Malicious emails will often have incorrect spelling or poor grammar, and many contain sentences that don't make sense. Some may just have a picture or a link in the content with no explanation (see example below).

We've also had examples where users have been sent SharePoint links, which just say: *'contact x has shared this folder with you'.*



From: A & L Electrical Solutions Limited <stacie@sfsme.com<mailto:stacie@sfsme.com>>
Sent: 16 April 2019 18:25
To: [redacted] <[redacted]<mailto[redacted]
Subject: A & L Electrical Solutions Limited - Invoice (SIN-237) for £3,310.00, due on 16/05/2019

A & L Electrical Solutions Limited

INVOICE SIN-237

TOTAL

£8,837.00

DUE DATE

16/05/2019

View Invoice <http://u284005.sfsme.com/156a1e43c3bce1ce>

Thank you for your business.
Full details, including payment terms, are included.
If you have any questions, please don't hesitate to contact us.
Kind regards,
A & L Electrical Solutions Limited

POWERED BY

[Sage Business Cloud]

Ask yourself:

'Am I being asked to send a payment or enter in my email credentials?'

'Have I been expecting this email?'

'Can I call someone or speak in person to verify the authenticity before clicking on the link?'

Spam emails come from compromised accounts

There can be instances where you'll be sent a spam email from a legitimate account. This can happen when an email account has fallen victim to a similar spam email and has been compromised.

These emails are perhaps the most difficult to spot as they'll come from a recipient, you're likely to have been in contact with before, however they do still have the following traits:

- Email will have very little personal information

- There will be a hyperlink of some sort in the email, a request for a bank transfer or an attachment

- The content may be incorrectly formatted or look unusual

Ask yourself:

'Could I call or speak to the sender in order to verify authenticity?'

'Have I been expecting this email?'

'Has anyone else also just received a link from this user?'

Number One Rule:

<u>NEVER</u> make any payment based on an email request without verifying it verbally.

If you are ever in any doubt whatsoever about the legitimacy of a specific email always forward the email across to support@ramsac.com

ramsac
the secure choice