A message from Catherine

Beware phishing scams

Dear Colleagues,

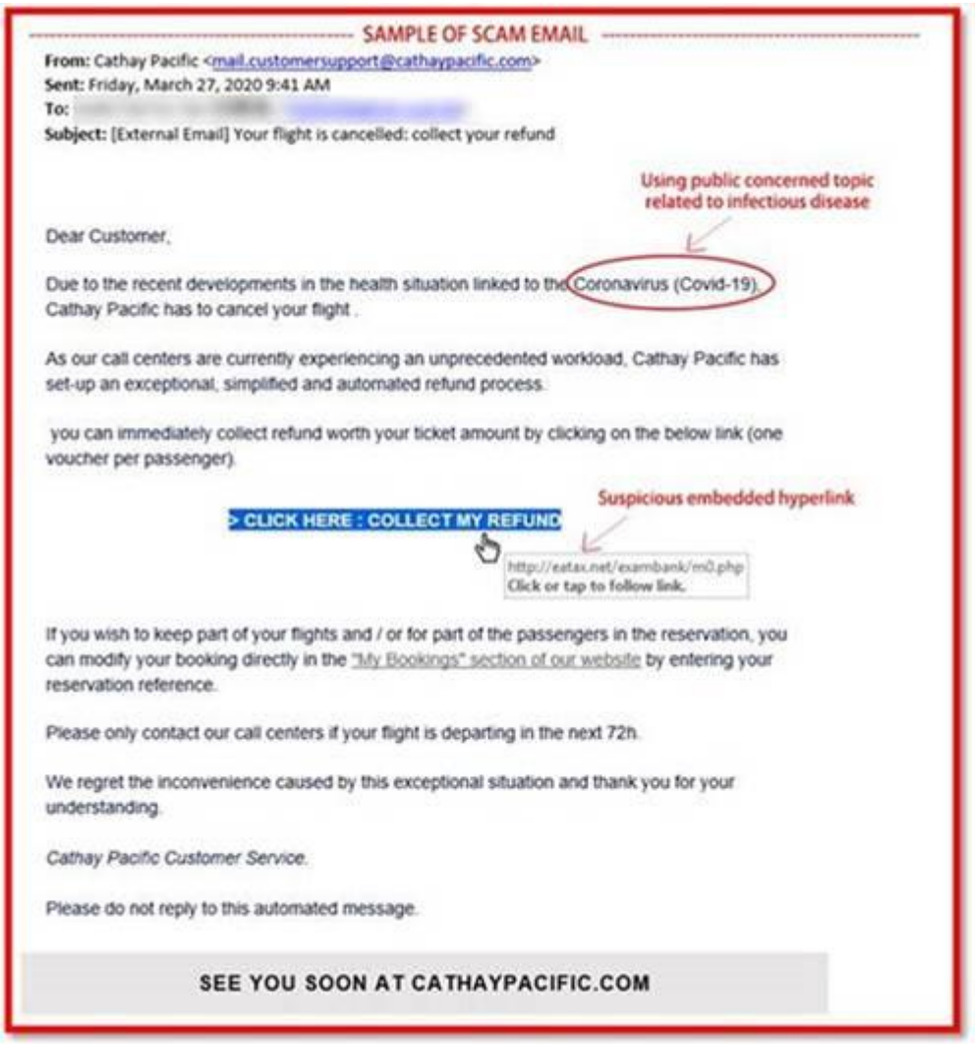
In the current environment as the COVID-19 crisis continues to unfold, we are seeing a rise in scams using the coronavirus as bait to carry out cyberattacks. It is vital that we all remain vigilant to protect ourselves from these scams.

Scammers are sending emails or messages linked with fake websites to make it appear that they are from an official institution or medical supplier. These scams, known as phishing attacks, are designed to steal personal data, spread malware and conduct money fraud.

Please find below top tips to protect your data:

- Verify the destination of embedded links by hovering the mouse pointer over the hyperlink without clicking it
- Never click any hyperlinks or opening any attachments provided in suspicious emails
- Beware of emails asking for sensitive data (e.g. account passwords or bank account information)
- Don’t trust emails simply because the sender’s email addresses are from someone with authority. Seek verification via telephone if in doubt. Use official contact channels or contact details that you already have on file.
- Check the sender’s email address carefully
- Do not visit suspicious and unknown web sites from your PC or mobile devices
- Report suspected scams to OCMS Service Desk (1800 773 475)
- Do not forward the phishing emails to other colleagues
- Install anti-malware software and keep it up to date
- Do not install mobile Apps from unknown sources
- Use well-known and secure Wi-Fi network only
- Use trusted websites for up-to-date, fact-based information about COVID-19

Scams can be very convincing as we can see in the example below. This phishing email is pretending to be from the airline Cathay Pacific. It exploits existing concerns around COVID-19, claiming to offer flight refunds.



It is okay to feel worried and concerned during this period of uncertainty, and that makes it important that we take time to understand if messages and emails are suspicious before clicking links and potentially compromising data security.

Thank you for your continued commitment and focus. Stay safe everyone.

Regards,

Catherine Baxter
Chief Operating Officer

METRO