



ASTONLARK

Five signs to spot a Coronavirus phishing email

1. Plays on fear and urgency

- Any legitimate source will speak in a calm and credible voice. Their email subject line won't be, "New Coronavirus Cases Confirmed in Your City" and the email won't ask you to click to learn about nearby "high-risk" areas.



2. Requests credentials, personal or financial information

- Think about it...why would a public health message send you to a webpage that requests your credit card number? It wouldn't. Major red flag.



3. Uses an unfamiliar greeting

- A recent Coronavirus phishing email began with "Sir/Madam" - a greeting that's very formal for today's business emails.



4. Has an unusual sender's address

- Another phishing email was supposedly from the 'International Civil Aviation Association'. Yet this email was sent from an 'aol.com' email address.



5. Contains spelling and grammatical errors

- "The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation." Be vigilant and careful when reading emails to spot spelling and grammar mistakes. They're not always noticeable at a quick glance.



For more information on cyber security, speak to our cyber specialists on **020 8633 8430**
www.astonlark.com/cyber

Source: Cofense - Coronavirus scams

Aston Lark Limited Registered in England and Wales No: 02831010
Registered office: Ibex House, 42-47 Minories, London EC3N 1DY
Aston Lark Limited is authorised and regulated by the Financial Conduct Authority.

AL-COM-017-0420

