KEEP CALM. DON'T CLICK.

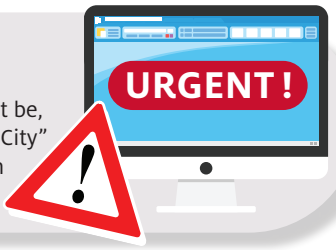
Whenever there's a major disaster, phishing emails are sure to follow. Cybercriminals prey on human emotions like fear and urgency, which today are as prevalent as the Coronavirus itself.

Here are 5 signs to spot a phishing email:

1

Plays on Fear and Urgency

Any legitimate sender will speak in a calm, 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

Asks for Credentials, Personal or Financial Information

Why would a public-health message send you to a webpage that wants your credit card number? It wouldn't. **Major red flag.**

3

Uses an Unfamiliar Greeting

One recent Coronavirus phish began with "Sir/ Madam" - a salutation that's weirdly formal for today's business emails. Again, it doesn't exactly scream trusted source.

4

Has a Sketchy Email Address

Another phish was supposedly from the International Civil Aviation Association. It contained no fewer than 5 links, inviting you to view Coronavirus impact stats or travel advisories. Yet this email had an **aol.com** email address. Um, no.

5

Makes Spelling or Grammar Errors

" The virus is speading like wide fire and the word health organization are doing everything possible to contain the current situation."
An obvious phishing email, though other writing mistakes are less noticeable.

Visit **uh.edu/covid19** for authoritative UHS information on the Coronavirus.

UNIVERSITY of HOUSTON SYSTEM
INFORMATION SECURITY