Cleveland Clinic

5 Signs a Coronavirus Email is a Phish

1 Plays on Fear and Urgency.

Any legit source 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.

Think about it. 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.

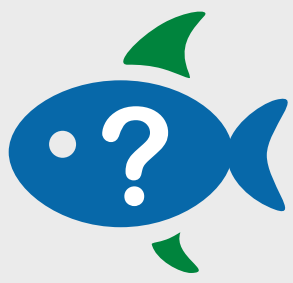
One recent Coronavirus phish began with "Sir/Madam"— a salutation that's weirdly formal for today's business emails. Again, it doesn't exactly scream trusted source.

4 Has a Sketchy Email Address.

Another phish was supposedly from the International Civil Aviation Association. It contained no fewer than 5 links, letting you 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 spreading like wide fire and the world health organization are doing everything possible to contain the current situation." An obvious phishing email, though other writing mistakes are less noticeable.



Let's work together to prevent cybersecurity incidents and protect our organization.

If you suspect a suspicious email, please use the Blue Fish button to report it. Send to phishtanktriage@ccf.org if you don't have the Blue Fish button or are on a mobile device.

For more information, review the PhishMe reporting toolkit on our cybersecurity intranet page.