Exploiting Novel Coronavirus (COVID-19):
Watch out for the Growing Number of Scams!

Security experts say a spike in email scams linked to Coronavirus is the worst they have seen in years.

Criminals are preying on fear and sending various scam emails related to COVID-19.

Below are some examples of the types of scams you should watch for:

1. **Emails that appear to be from organizations** such as the CDC (Centers for Disease Control), or the WHO (World Health Organization). Criminals have crafted emails that appear to come from these sources, but they **contain malicious phishing links or dangerous attachments**.

2. **Emails that ask for charity donations** for studies, doctors, or victims that have been affected by COVID-19. Criminals often create fake charity emails after global phenomena occur (natural disasters, health scares, etc.).

3. **Emails that claim to have a “new” or “updated” list of cases** of Coronavirus in your area. These emails could contain **dangerous links** and information designed to scare you into clicking on the link.

Remain cautious! Always remember there are ways to protect yourself from these scams:

- **Never** click on links or download attachments from an email that you weren’t expecting.

- **Report** – If you receive a suspicious email that appears to come from an organization, report the email separately to the official organization directly through their website. Type the organization’s web address in your browser instead of clicking on any links in emails or other messages.

- **Donations** – If you want to make an online charity donation, go to the individual charity website of your choice to submit your payment. Make sure it is a secure payment website. Type the charity’s web address in your browser instead of clicking on any links in emails or other messages. You can also mail a check to a local charity you trust.