COVID-19 is leading to an increase in email phishing attempts.

Be aware. Be prepared.

DOES THE EMAIL...

- **Demand "immediate action" before something bad happens**
  ("I will infect your family with the coronavirus")
- **Have a generic greeting**
  ("Dear Sir or Madam...")
- **Request highly sensitive info**
  (e.g. credit card number, SS ID or password)
- **Look like it is from a trusted source or company, but uses a personal email address**
  (i.e. @gmail.com; think banks, Amazon, etc.)
- **Simply ask you to reply to their email**
  (Some scammers wait until you are "hooked" to share their request.)
- **Come from someone you know but contain wording that does not sound like the sender**
  (Spelling / grammar mistakes; phrases they wouldn't use)
- **Offer money for placing a URL in a prominent place**
  (such as in a comment under a YouTube video)

IF YOU ARE SUSPICIOUS, CALL THE SENDER TO VERIFY THEY SENT IT OR DELETE THE EMAIL!

AgeRight.org

AgeRight.org