



The COVID-19 crisis creates an increased opportunity for cyber criminals to target you or your practice. These cyber threat actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes.

Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

Cyber threat actors may also try to benefit from the situation by using Spear Phishing techniques. Spear Phishing means criminals personalize their attacks specifically to you. They find out information about you and create a tailored scam that looks legitimate, even calling you by name. Often these have real people behind them, so responses can be very specific and tailored.

Here are some tips to identify a phishing email:

- Does the message trigger an emotional reaction such as curiosity or fear, or does it try to pressure you?
- Does it ask you to click on a link, open an attachment or provide personal information?
- Do you know the sender? Hackers sometimes spoof a sender's email address to make the mail look like it comes from someone you know. Check the email is really from the person it says it is from. Make sure you verify the email address. Don't just look at the name.
- Is the email asking you to do something financial or making a request that isn't typical behavior of the sender?
- Were you expecting this email? If the answer is "No" - DO NOT act on the request. If it doesn't look or sound right, it probably isn't right. When in doubt, pick up the phone and call the person who sent it to you. Nothing is so urgent that it cannot wait for verification.

Below are reputable sources with information on avoiding and preventing scams and phishing emails related to COVID-19. There are also additional links for general computer safety.

<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

<https://www.consumer.ftc.gov/blog/2020/04/avoiding-ssa-scams-during-covid-19>

<https://www.consumer.ftc.gov/blog/2020/04/scammers-are-using-covid-19-messages-scam-people>

<https://www.cdc.gov/media/phishing.html>

<https://www.eff.org/deeplinks/2020/03/phishing-time-covid-19-how-recognize-malicious-coronavirusphishing-scams>

<https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email>

<https://staysafeonline.org/>

<https://www.us-cert.gov/home-and-business>