Coronavirus Scams

Criminals are exploiting those fearful of COVID-19.

Today, this includes people mostly over the age of 65. Criminals are aware of this fact and that the radar of online scammers has moved towards the market of COVID-19 awareness.

A study published in the Journal of applied psychology shows that people are more willing to share personal information, such as their email address, when it comes to the COVID-19 pandemic.

While many fear scams, it is critical to be aware of how to protect yourself from these scams. The following is a list of tips to protect yourself from COVID-19 related phishing attacks.

Phishing Scams.

1. Confirm who sent the message:
Coronavirus phishing scams can be transmitted via email or social media, including Facebook, Instagram, Twitter, and others.

2. Watch out for telltale signs:
Suspicious signs or words is a telltale sign for anyone who is communicating without knowing the_experts.

   a. Request for personal information.
   b. Unrelated or spam messages.
   c. Requests for donations to emergency response funds.

3. Get real information:
There are several resources that the WHO website is the top destination to find information about COVID-19. You can also see if the website uses a secure connection by looking for the lock symbol in the browser address bar.

What Coronavirus phishing scams look like

1. Addressees send messages with self-promotion.

2. A Coronavirus alert will usually look like an appeal for contributions on social media.

3. The body of an email will look like a news article.

4. Requests for donations have been made to emergency response funds.

5. The website is not secure.

6. The message is not relevant.

7. The message is not urgent.

8. The message uses a spam word.

9. The message is not a news article.

10. The message does not direct you to anything.

Protecting yourself

1. Confirm who sent the message:
Coronavirus phishing scams can be transmitted via email or social media, including Facebook, Instagram, Twitter, and others.

2. Watch out for telltale signs:
Suspicious signs or words is a telltale sign for anyone who is communicating without knowing the_experts.

   a. Request for personal information.
   b. Unrelated or spam messages.
   c. Requests for donations to emergency response funds.

3. Get real information:
There are several resources that the WHO website is the top destination to find information about COVID-19. You can also see if the website uses a secure connection by looking for the lock symbol in the browser address bar.

If you find yourself in a situation where you are unsure about the authenticity of a message, contact the relevant authorities or organizations to verify the information.