SET SEG

COVID-19
PHISHING ATTACKS AWARENESS

The coronavirus is changing our lives and, as a result, people are reaching out for information, safety and support. Organized crime groups are exploiting this fear and uncertainty by launching COVID-19 themed spear-phishing attacks, luring targets to fake websites seeking to collect Office 365 credentials.

Build your awareness and ability to recognize a phishing attack by reviewing the examples below.

- **Malicious Microsoft Documents Attached to Emails**

  COVID-19 themed phishing emails with attachments made up of malicious Microsoft documents can exploit a known Microsoft vulnerability to run malicious code. Macro-enabled Microsoft Word documents containing health information can trigger the download of Emotet or Trickbox malware.

- **Luring Users to Fake Websites to Gather Information**

  Phishing emails lure targets to fake copies of the Center for Disease Control website which solicits user credentials and passwords.

- **Malware Downloads Disguised As System Updates**

  A selection of phony customer advisories claim to provide customers with updates on service disruption due to COVID-19 and instead lead to downloading malware. Some emails even claim to come from various government Ministries of Health or the World Health Organization and provide precautionary measures, but again lead to embedding malware.

- **COVID-19 Tax Rebate Claim**

  COVID-19 tax rebate phishing encourages recipients to browse a fake website and collects financial and tax information from unsuspecting users.

- **Offering Giveaways Through Health Updates**

  Many existing organized crime groups have changed tactics, using materials that share health updates, such as fake cures, fiscal packages, emergency benefits and supply shortages. Typical suspicious email characteristics include:

  - Poor grammar, punstuation, and spelling
  - Unexpected design and poor email quality
  - Uses of terms such as “Dear Colleague,” “Dear Friend,” or “Dear Customer,” instead of addressing you by name
  - A veiled threat or a false sense of urgency
  - Direct requests for personal or financial information