Protect yourself from COVID-19 scams

Among the threats posed by the COVID-19 outbreak are scams aimed at exploiting fears and spreading disinformation about the pandemic. For example, individuals and businesses using the internet to sell fake cures for COVID-19, market products falsely claiming to mitigate COVID-19, and fraudulently retail COVID-19 supplies, such as face masks and hand sanitizer.

In addition there are reports of phishing emails from entities posing as the World Health Organization or the Centers for Disease Control (CDC) and reports of malware being inserted onto mobile apps designed to track the spread of the virus.

Defending Against COVID-19 Cyber Scams

The Cybersecurity and Infrastructure Security Agency (CISA) warns individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Cyber 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.

CISA encourages individuals to remain vigilant and take the following precautions.

- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Use trusted sources--such as legitimate, government websites--for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.
- Review CISA Insights on Risk Management for COVID-19 for more information.

Some examples of scams include:

- Individuals and businesses selling fake cures for COVID-19 online and engaging in other forms of fraud.
- Phishing emails from entities posing as the World Health Organization or the Centers for Disease Control and Prevention.
- Malicious websites and apps that appear to share Coronavirus-related information to gain and lock access to your devices until payment is received.
- Seeking donations fraudulently for illegitimate or non-existent charitable organizations.
- Medical providers obtaining patient information for COVID-19 testing and then using that information to fraudulently bill for other tests and procedures.

Attorney General William P. Barr is urging the public to report suspected fraud schemes related to COVID-19 (the Coronavirus) by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721) or by e-mailing the NCDF at disaster@leo.gov.

Content from: U.S. Department of Justice and Department of Homeland Security