Chicago Police Department

Crime Prevention & Information Center

Private Sector Situational Awareness Bulletin

(U) Situational Awareness
COVID-19 CYBER SECURITY ALERT

Please be aware of phishing email campaigns related to COVID-19. **Use caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink**. Additionally, please be cautious of any social media posts, texts, or phone calls related to COVID-19. Malicious actors are likely to take advantage of the COVID-19 national state of alert to send emails with attachments or URL links to websites disguised to deceive people into revealing sensitive information or donating to fraudulent charities or causes.

The CPIC encourages the following precautions as outlined by the Federal Cybersecurity and Infrastructure Security Agency (CISA):

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See CISA's Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.

- Use trusted sources, such as government websites for information about COVID-19:
  http://chicago.gov/coronavirus
  http://cdc.gov/coronavirus

- 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.
  https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams

- Be cognizant of your organization's "EXTERNAL EMAIL WARNING" banner to help you identify if emails are being "spoofed" to look like they are coming from within the organization:

(U) Additional links for Cyber Awareness.

https://www.dhs.gov/about-stopthinkconnect
https://www.dhs.gov/national-cyber-security-awareness-month
https://www.us-cert.gov/bsi/best-practices
https://www.cisa.gov/cyber-essentials

See Something…Say Something…Call 911 IMMEDIATELY