
Health Emergency Exploited by Phishing Campaigns

Medical Device Special Report - Published 3/20/2020

Geographic Regions
Worldwide

Suggested Distribution
Clinical/Biomedical Engineering, Information Technology

Problem
— The COVID-19 health emergency is being exploited by phishing and malicious misinformation campaigns.
— Phishing e-mails seeming to contain COVID-19-related content attempt to compromise credentials or spread malware.

This alert is a living document and may be updated when ECRI receives additional information.

Recommendations
— Ensure that e-mail filtering and anti-malware systems are kept up to date.
— Educate users on phishing awareness, including new COVID-19-related misinformation campaigns.

Background
— Malicious actors are exploiting the COVID-19 health emergency with targeted phishing e-mails falsely claiming to contain COVID-19-related content.
— Phishing campaigns exploiting the crisis include the following:
  • Spoofing official COVID-19-related communication from your organization
  • Spoofing IT communications targeting employees working from home
  • Spoofing COVID-19-related communications from government entities and public health organizations

References