| | | | | | |
|---|---|---|---|---|---|
| **Accession Number:** | H0570 | **ECRI Priority:** | High | **Published:** | 03/20/2020 |
| **Channel:** | Devices | **FDA:** | Not Specified | **Last Updated:** | 03/20/2020 |

**[COVID-19] Health Emergency Exploited by Phishing Campaigns [ECRI Exclusive Hazard Report]**

## Problem

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

### ECRI Recommendations:

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

### Background:

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

### References


1. United States. Department of Homeland Security. Cybersecurity and Infrastructure Security Agency. Defending against COVID-19 cyber scams [online]. 2020 Mar 6 [cited 2020 Mar 20]. Available from Internet: Click here.
2. Ars Technica. The Internet is drowning in COVID-19-related malware and phishing scams [online]. 2020 Mar 16 [cited 2020 Mar 20]. Available from Internet: Click here.


## Geographic Region(s)

Worldwide

## Suggested Distribution

Clinical/Biomedical Engineering, Information Technology

## Comment

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