akerman

Blog Post

# New FBI Alert to Healthcare Providers – Beware of COVID-19 Phishing Campaigns

April 27, 2020
By Elizabeth F. Hodge and Christy S. Hawkins

Healthcare providers are under siege, not only from the COVID-19 pandemic, but also from cyber criminals. Following reports of targeted email phishing attempts, the FBI issued a FLASH alert warning healthcare providers on April 21, 2020, that they are at heightened risk for cyber attacks that use COVID-19 as bait. The FBI's FLASH alert follows its repeated alerts about cyber attacks exploiting COVID-19, including online scams, advance fee and business email compromise scams, cryptocurrency scams, health care fraud schemes, money mule schemes, and exploitation of the increased use of virtual environments.

As we previously reported cyber criminals are using evolving, sophisticated attacks that seek to exploit the state of emergency caused by the pandemic by sending emails and SMS messages claiming to have urgent information on COVID-19. On March 18, 2020, network perimeter security tools of U.S.-based healthcare providers identified email phishing attempts from domestic and international IP addresses. Those phishing emails contained subject lines related to COVID-19 and included malicious files as attachments in the form of Microsoft Word files, ZIP files, Microsoft Visual Basic Script, Java, and Microsoft Executables, among others. The FBI said it is likely these attachments would have created a gateway into the healthcare providers' information

## Related People

Christy S. Hawkins
Elizabeth F. Hodge

## Related Work

Healthcare
Data Privacy and Security

## Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

## Coronavirus Resource Center

Visit the Resource Center

systems to enable further exploitation, persistence and exfiltration of data. More information on indicators of the suspicious emails is available in the FLASH alert.

To help healthcare IT professionals thwart these phishing attempts, the FLASH alert lists the indicators of compromise and hashes used in COVID-19 phishing scams to date. It is critical that healthcare providers arm their employees with the information needed to recognize these attacks.

The FLASH alert requests that providers who are targeted by a phishing campaign send the FBI a copy of the email with the full email header and a copy of any attachments. If a provider is a victim of a cyber intrusion as a result of phishing attack, it should keep any logs, images of infected devices, and, if possible, memory capture of all affected equipment.

To help prevent successful phishing campaigns, healthcare providers can do the following:

- Be alert to unsolicited email attachments, even from senders known to the recipient. If the sender appears to be someone known to the recipient, contact the sender to confirm the legitimacy of the attachment.
- Keep software up to date. Maintain a regular schedule to stay current on software patches and updates.
- Recipients should not open emails or email attachments that seem suspicious, even if the provider's software patches are current.
- Save and scan any attachments before opening them.
- Turn off the option to automatically download email attachments.

Also, even if formal phishing testing and training isn't feasible due to constraints created by the COVID-19 pandemic, providing staff with short alerts

and reminders may make the difference between an organization that falls victim to a cyber attack and one that can continue to focus its critical attention on saving lives during the COVID-19 global emergency.

The FBI, the Department of Homeland Security, and the Department of Justice have provided, and continue to provide, even more tips for organizations to protect themselves. By keeping staff informed and on the lookout for potential phishing scams, organizations can take an important step to protect themselves against cyber attackers attempting to exploit COVID-19.

---