HHS Office for Civil Rights in Action

April 30, 2020
COVID-19 Cyber Threat Resources

Cyber-criminals may take advantage of the current COVID-19 global pandemic for their own financial gain or other malicious motives. However, resources are available to raise awareness of COVID-19 related cyber threats and help organizations detect, prevent, respond, and recover from these threats. Below are resources that may be of interest to the healthcare community.

Cyber Attack Quick Response Checklist: Following the WannaCry ransomware attack in 2017, the HHS Office for Civil Rights (OCR) developed a checklist and corresponding Infographic that identifies the steps for a HIPAA covered entity or business associate to take in response to a cyber-related security incident. With the increase in COVID-19 related malicious activity, HIPAA covered entities and business associates are encouraged to review this checklist and infographic for steps to take in the event it encounters a cyber-related security incident.

COVID-19 Email Phishing Against U.S. Healthcare Providers: The FBI issued a notice regarding email phishing attempts targeting healthcare providers. These phishing attempts leverage COVID-19 related subject lines and content in an attempt to distribute malicious attachments. The notice includes information on how to identify specific phishing attacks and recommends actions to take when such attacks are encountered.

Online Extortion Scams Increasing During The Covid-19 Crisis: The Internet Crime Complaint Center (IC3) released an advisory regarding an increase in reports of online extortion scams. This advisory includes information on how to recognize online extortion scams and steps to take protect oneself from these scams.

Selecting and Safely Using Collaboration Services for Telework: Due to the COVID-19 global pandemic, many people are working from home using various video conferencing and online collaboration tools. The National Security Agency (NSA) published a notice that includes criteria to consider when selecting an online collaboration tool as well as information on how to use online collaboration tools securely.

COVID-19 VTC Exploitation: The increased use of video conferencing and online collaboration tools has led to an increase in malicious activity seeking to exploit the unsecure use of these tools. The HHS Health Sector Cybersecurity Coordination Center (HC3) released a white paper outlining ways these tools could be exploited and recommendations to mitigate these issues.

COVID-19 Cyber Threats: The HC3 also produced a brief on COVID-19 related cyber threats. This brief includes details on the increase in COVID-19 related malicious activity as well as information on how COVID-19 themed phishing attacks and websites are used as lures to trick users into downloading malicious software or directing users to malicious websites.

OCR's Cyber Security Guidance Material may be found here: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html. For more information related to HIPAA and COVID-19, please visit: https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html.