WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 68, Issue 28

Thursday, July 11, 2024

M3 Insurance Continues to Keep WHA Members Up To Date on Cybersecurity

The FBI and HHS released a joint Cyber Security Advisory notice notifying providers of a new social engineering campaign targeting health care providers.

According to the notice issued by the FBI and HHS, "threat actors are using phishing schemes to steal login credentials for initial access and the diversion of automated clearinghouse (ACH) payments to US controlled bank accounts. Healthcare organizations are attractive targets for threat actors due to their size, technological dependence, access to personal health information, and unique impacts from patient care disruptions. The FBI and HHS encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of social engineering incidents."

The notice also outlines that the threat actors are gaining access through social engineering or phishing methods by calling the IT Help Desk in an attempt to reset passwords, bypassing MFA, etc. They are using voice over Internet protocol (VoIP) numbers to conduct these campaigns as well. The list of phone numbers used by threat actors is also provided in this advisory.

Risk Management Recommendations

- Implement multi-factor authentication (MFA) for every account.
- Train IT Help Desk employees on this vulnerability. MFA bypasses should not be allowed for any individual calling into the Help Desk.
- Reduce threat of malicious actors using remote access tools by:
  - Auditing remote access tools on your network to identify currently used and/or authorized software.
  - Reviewing logs for execution of remote access software to detect abnormal use of programs running as a portable executable
  - Using security software to detect instances of remote access software being loaded only in memory.
  - Requiring authorized remote access solutions to be used only from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
  - Blocking both inbound and outbound connections on common remote access software ports and protocols at the network perimeter.
  - Applying recommendations in the Guide to Securing Remote Access Software.
- Organizations are urged to check phone call logs to identify if their organization has been in contact with any of the phone numbers listed in the Advisory Notice. If contact was made, the organization should assess what access the UA was given and if the UA was successful in accessing sensitive information.

Other Articles in this Issue