CARLTON FIELDS

HHS Warns Health Care Sector of AI-Driven Phishing, Social Engineering Attacks on IT Help Desks

April 25, 2024

The Department of Health and Human Services recently issued a health sector alert through the Health Sector Cybersecurity Coordination Center (HC3). HC3 warns health sector organizations of new, sophisticated cybersecurity threat techniques that use publicly available information and generative artificial intelligence to target health care organizations' IT help desks. This alert follows the widely publicized ransomware attack on Change Healthcare and separate attacks on IT help desks at MGM Resorts International and Caesars Entertainment. Each incident resulted in widespread business outages and significant financial losses. Threat actors are increasingly targeting help desks with novel, complex attacks. They impersonate health care leaders, tricking help desks into providing them with remote access to email accounts. For instance, threat actors have used information obtained from "professional networking sites" and "other publicly available information sources such as previous data breaches" to impersonate health care employees, specifically employees in revenue cycle or administrator roles. On such a call with a corporate help desk, the threat actor will convince the employee to add a threat actor controlled device to multifactor authentication accounts, enabling access to a real employee's email account. Once there, the threat actor can divert payments to U.S. bank accounts under the threat actor's control, and eventually transfer the funds to an offshore account. The alert also describes "spearphishing voice" or "vishing" attacks whereby threat actors leverage generative voice AI technology to impersonate employees' voices while requesting help desk assistance, adding further complexity to threat detection. In data cited by HC3, and in the authors' experience, voice AI-based scams are on the rise, and pose a new challenge for health care security personnel and managers of help desk employees. In addition to releasing sector alerts with threat intelligence, HHS can and does investigate and penalize companies that, in its view, fail to adequately safeguard protected health information.

Failure to implement appropriate administrative and technical safeguards (e.g., policies and procedures to verify and authenticate individuals seeking access to electronic protected health information) can result in HHS investigations and fines. For example, HHS extracted a $1.25 million settlement with an Arizona-based health care system in 2023. In that settlement, the HHS investigation concluded, in part, that the entity had failed to implement procedures to verify that persons or entities seeking access to ePHI were who they claimed to be, in accordance with 45 C.F.R. § 164.312(d). HHS has signaled that it intends to expand both its regulation and enforcement of cybersecurity standards. According to its latest strategy publication, the Centers for Medicare & Medicaid Services will propose new cybersecurity requirements for hospitals through Medicare and Medicaid. The agency has also committed to "work with Congress to increase civil monetary penalties for HIPAA violations." For those hospitals that have been the victims of criminal cyberattacks on themselves or their vendors, despite having industry-standard protections in place, the idea that the government response to this crisis is additional regulation and larger potential fines will be of little comfort and much consternation. Additionally, data security events impacting PHI can lead to private lawsuits, ensuing litigation costs, and, in some cases, multimillion-dollar settlements. When faced with the escalating sophistication of cyberattacks and the threat of lawsuits and regulatory enforcement, organizations can take actionable steps to mitigate these threats. Below are a few ideas to consider as part of an organization's planning:

- Conduct periodic training with employees, including social engineering training, to increase awareness of emerging techniques and how to report incidents to the appropriate internal personnel promptly.
- Review cybersecurity policies and procedures to enhance verification and authentication for account access, including controls around changes to multifactor authentication methods.
- Consider social media use policies to limit the amount of information employees make publicly available via social media or, barring that, educate employees about the risks from such exposure.
- Enhance help desk procedures to verify and confirm reported issues (e.g., require callbacks to the employee's phone number on record for certain escalated requests), and then audit and train help desk employees on these procedures.
- Revisit SMS as an MFA option and consider if an authenticator mobile app could provide improved security.
- Assess the number of administrator credentials outstanding and whether technical controls can be improved, including limiting or eliminating off-site admin access.

Authored By

John E. Clabby

Michael A. Bailey

Related Practices

Cybersecurity and Privacy
Health Care

Related Industries

Health Care