FINISHED INTELLIGENCE REPORTS

CISA: Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication

TLP:WHITE

Nov 01, 2022

On October 31, 2022, the Cybersecurity Infrastructure Security Agency (CISA) released two fact sheets highlighting threats against accounts and systems using certain forms of multifactor authentication (MFA). CISA strongly urges all organizations to implement phishing-resistant MFA to protect against phishing and other known cyber threats. If an organization using mobile push-notification-based MFA is unable to implement phishing-resistant MFA, CISA recommends using number matching to mitigate MFA fatigue. Although number matching is not as strong as phishing-resistant MFA, it is one of the best interim mitigation for organizations that may not immediately be able to implement phishing-resistant MFA.

Health-ISAC is sharing the following information in conjunction with a previously distributed bulletin on Threat Actors Using MFA Fatigue Attack to Defeat Advanced Authentication Methods.

Health-ISAC encourages members to review the fact sheets below regarding information pertaining to multifactor authentication.

CISA recommends users and organizations see CISA fact sheets Implementing Phishing-Resistant MFA and Implementing Number Matching in MFA Applications.

Visit CISA.gov/MFA for more information on MFA, including an infographic of the hierarchy of MFA options.

Reference(s)	CISA

Alert ID 5b53f3d2

This Alert has 2 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags Cyber Threats, MFA, CISA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**