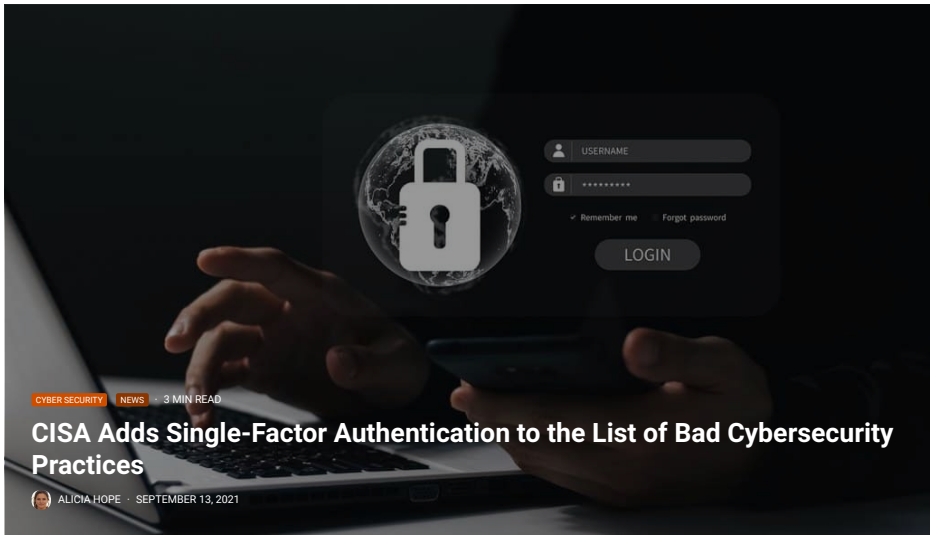


The Cybersecurity and Infrastructure Security Agency (CISA) announced the addition of single-factor authentication to the list of bad practices. This authentication method relies on matching a simple attribute, like a username to a password.

According to the agency, the method poses significant cybersecurity risks especially to organizations dealing with management, critical infrastructure, and secure national functions.

CISA discourages risky cybersecurity practices like single-factor authentication

CISA says that single-factor authentication is among the most exceptionally risky cybersecurity practices for remote or administrative access.

"Single-factor authentication is a common low-security method of authentication. It only requires matching one factor such as a password to a username to gain access to a system," CISA wrote. "Although these Bad Practices should be avoided by all organizations, they are especially dangerous in organizations that support Critical Infrastructure or National Critical Functions."

Other appalling cybersecurity practices include using default passwords and credentials and obsolete/unsupported/end-of-life software.

However, the current list of bad cybersecurity practices isn't comprehensive. Other poor cybersecurity practices that CISA discourages include:

- Using weak cryptographic functions or key sizes
- Flat network topologies
- Mixing IT and OT networks
- The lack of least privilege making everyo
- Reuse of previously compromised systen
- Transmission of sensitive, unencrypted/unauthenticated traffic over uncontrolled networks
- Poor physical access controls

The agency encouraged organizations to engage in critical conversations to address bad cybersecurity practices like using single-factor authentication. CISA also referred users to the CISA Capacity Enhancement Guide: Implementing Strong Authentication guidebook to assist them in implementing strong authentication.

Threat actors have invented ingenious methods of harvesting username and passwords combinations through various methods like phishing and exploiting vulnerabilities.

According to CISA, single-factor authentication was extremely vulnerable to various attacks, including brute force, phishing, social engineering, keylogging, network sniffing, malware, and credential dumping. Password reuse, admin password sharing, and storage of plaintext passwords also made single-factor authentication more vulnerable to compromise.

Similarly, many organizations have appalling cybersecurity practices as demonstrated in the numerous high-profile data breaches experienced recently. Consequently, single-factor authentication has become an unreliable method of proving identity.

"The fact that the Critical Infrastructure Security Association has outlined bad practices that shouldn't be followed in securing critical infrastructure is a great thing, but it seems like these are cybersecurity 101 facts that everyone knows," Anurag Gurtu, CPO at StrikeReady, said. "An effective strategy may include providing free or heavily discounted software to guide organizations through an audit and find these problems, or partnering with Hi-Tech companies to create software to handle this task." Most authentication methods depend on something you know (knowledge), for example, a password, something you have, for example, a smartcard or OTP, and something you are, for example, physical characteristics like

fingerprints.

Although single authentication used two factors, i.e., username and password combinations, they all belonged to the same category hence becoming a single-factor authentication.

According to the bureau, adding another authentication factor increases the difficulty of compromising an account. Also known as two-factor authentication (2FA) or multi-factor authentication (MFA), this method requires two or more factors from different categories, for example, something you have and something you know.

According to a joint Google, New York University and University of California San Diego study referred to by CISA, multi-factor authentication blocks 100% of automated attacks, 99% of bulk phishing attacks, and 66% of targeted attacks on Google accounts.

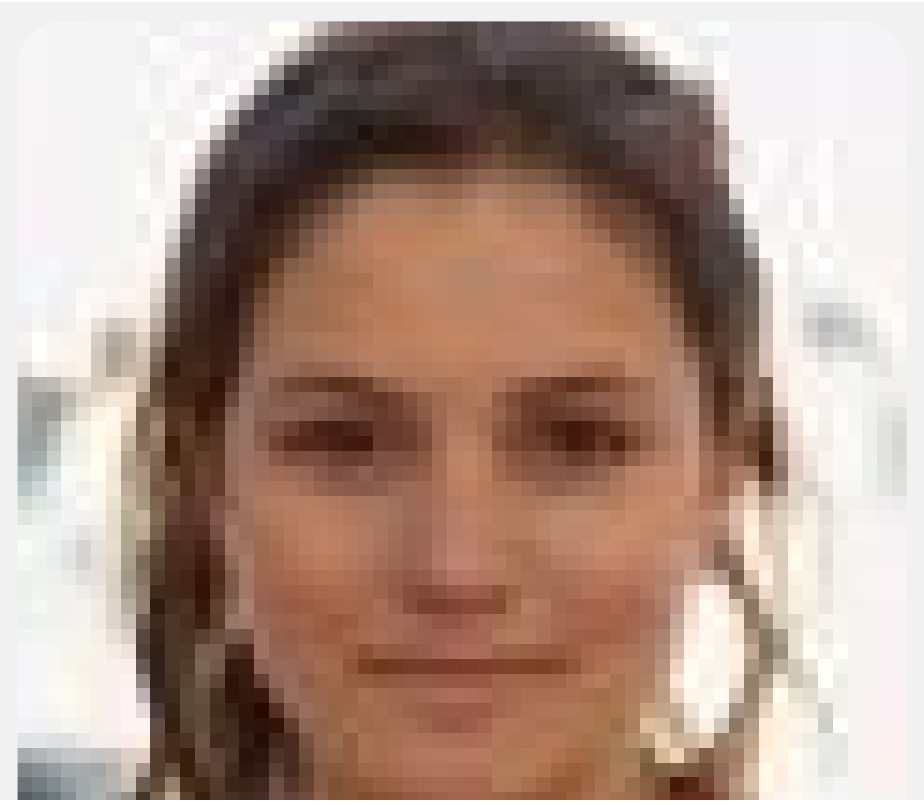
"To receive the full benefit of an MFA capability, organizations should be sure to implement it across all systems, applications, and resources," CISA wrote. "Requiring multi-factor authentication to gain initial access to an organization's network (usually the user's workstation) is a good first step; however, this provides only limited protection to other systems and data within the organization that are protected with only single-factor authentication."

CISA recommended that organizations expand multi-factor authentication to other methods that authenticate users across systems, applications, and resources without requiring individual MFA implementations at each step.

Another benefit of these methods is that they allow revocation of access centrally by an identity management administrator once an employee leaves the organization. They also simplify user experience because employees do not have to track multiple identities across applications. Thus, the bureau recommended single sign-on (SSO) and identity federation services, noting that most applications shipped with SSO connectors already in place.

CISA, however, advised organizations to "know when to move on" when authentication solutions proved very expensive or too complicated. In such cases, they should implement compensating controls or migrate to new solutions that seamlessly integrate with strong authentication solutions.

TAGS #CYBERSECURITY PRACTICES #PASSWORDS #SINGLE FACTOR AUTHENTICATION



Alicia Hope

Staff Correspondent at CPO Magazine

Alicia Hope has been a journalist for more than 5 years, reporting on technology, cyber security and data privacy news.

LATEST

LEARN MORE

About
Contact
Our Advertising
Privacy Policy
Cookie Policy
Terms of Use

STAY UPDATED

Get notified of new articles and relevant events.

Type your email

I agree to the privacy policy

SUBMIT

CPO MAGAZINE

News, insights and resources for data protection, privacy and cyber security professionals.

LEARN MORE

About
Contact
Our Advertising
Privacy Policy
Cookie Policy
Terms of Use
Do Not Sell My Data

STAY UPDATED

Get notified of new articles and relevant events.

Type your email

I agree to the privacy policy

SUBMIT

FOLLOW US