
# Implementing Phishing-Resistant MFA

October 2022

## OVERVIEW

This fact sheet is intended to provide for IT leaders and network defenders an improved understanding of current threats against accounts and systems that use multifactor authentication (MFA). MFA is a security control that requires a user to present a combination of two or more different authenticators (something you know, something you have, or something you are) to verify their identity for login. MFA makes it more difficult for cyber threat actors to gain access to networks and information systems if passwords or personal identification numbers (PINs) are compromised through phishing attacks or other means. With MFA enabled, if one factor, such as a password, becomes compromised, unauthorized users will be unable to access the account if they cannot also provide the second factor. This additional layer ultimately stops some of the common malicious cyber techniques, such as password spraying.

CISA has consistently urged organizations to implement MFA for all users and for all services, including email, file sharing, and financial account access. MFA is an essential practice to reduce the threat of cyber threat actors using compromised credentials to gain access to and conduct malicious activity on networks. However, not all forms of MFA are equally secure. Some forms are vulnerable to phishing, "push bombing" attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM Swap attacks. These attacks, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems.

This fact sheet provides an overview of threats against accounts and systems that use MFA and provides guidance on implementing phishing-resistant MFA, which is the most secure form of MFA. CISA strongly urges all organizations to implement phishing-resistant MFA as part of applying Zero Trust principles. **Note**: The Office of Management and Budget requires agencies to adopt phishing-resistant MFA methods. While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort

## CYBER THREATS TO MFA

Cyber threat actors have used multiple methods to gain access to MFA credentials:

- **Phishing.** Phishing is a form of social engineering in which cyber threat actors use email or malicious websites to solicit information. For example, in a widely used phishing technique, a threat actor sends an email to a target that convinces the user to visit a threat actor-controlled website that mimics a company's legitimate login portal. The user submits their username, password, as well as the 6-digit code from their mobile phone's authenticator app.
- **Push bombing (also known as push fatigue).** Cyber threat actors bombard a user with push notifications until they press the "Accept" button, thereby granting threat actor access to the network.
- **Exploitation of SS7 protocol vulnerabilities.** Cyber threat actors exploit SS7 protocol vulnerabilities in communications infrastructure to obtain MFA codes sent via text message (SMS) or voice to a phone.
- **SIM Swap.** SIM Swap is a form of social engineering in which cyber threat actors convince cellular carriers to transfer control of the user's phone number to a threat actor-controlled SIM card, which allows the threat actor to gain control over the user's phone

## RECOMMENDED IMPLEMENTATIONS

Table 1 lists forms of MFA from strongest to weakest based on their susceptibility to the above cyber threats:

***Table 1: MFA Forms, Strongest to Weakest***

| Authentication Form | Overview | Threat |
|---|---|---|
| **Phishing-resistant MFA:**<br>• **FIDO/ WebAuthn authentication**<br>• **Public key infrastructure (PKI)-based** | Phishing-resistant MFA is the gold standard for MFA. See the Phishing-Resistant MFA Implementations section for more information.<br>CISA strongly urges system administrators and other high-value targets to implement or plan their migration to phishing-resistant MFA. | Resistant to phishing.<br>Push bombing, SS7, and SIM swap attacks are not applicable. |
| **App-based authentication:**<br>• **One-time password (OTP)**<br>• **Mobile push notification with number matching**<br>• **Token-based OTP** | App-based authenticators verify a user's identity either by generating OTP codes or by sending "push" pop-up notifications to the mobile application.<br>In mobile push notification, the user accepts a "push" prompt sent to the mobile application to approve an access request. When numbers matching is implemented, there is an additional step between receiving and accepting the prompt: the user is required to enter numbers from the identity platform into the application to approve the authentication request. See CISA fact sheet Implement Number Matching in MFA Applications for more information.<br>Token-based authenticators verify a user's identity by generating OTP codes that the user enters to prove possession of the token.<br>Authentication via app- or token-based OTP or mobile push with number matching are the best options for small- and medium-size business that cannot immediately implement phishing-resistant MFA. | Vulnerable to phishing attacks.<br>Resistant to push bombing.<br>SS7, and SIM swap attacks are not applicable |
| **App-based authentication:**<br>• **Mobile application push notification without number matching** | In standard mobile app push notification without number matching, the user opens and accepts a "push" prompt sent to the mobile application to approve an access request. There is no additional step between receiving and accepting the prompt. | Vulnerable to push bombing attacks as well as user error.<br>SS7 and SIM swap attacks are not applicable. |
| **SMS or Voice** | SMS or voice MFA works by sending a code to the user's phone or email. The user then retrieves this second factor code from their text or email inbox to use for login authentication.<br>This form of MFA should only be used as a last resort MFA option. However, it can serve as a | Vulnerable to phishing, SS7, and SIM swap attacks. |

| | | |
|---|---|---|
| | temporary solution while organizations transition to a stronger MFA implementation. | |

As part of long- and intermediate-term plans to apply Zero Trust principles, CISA encourages all organizations to implement phishing-resistant MFA. CISA recognizes that some applications or use cases may not allow for immediate implementation of phishing-resistant MFA. Organizations that have existing MFA systems that are not phishing-resistant should employ additional prevention and detection controls, such as number matching, as outlined in CISA fact sheet Implement Number Matching in MFA Applications.

CISA recommends that organizations identify systems that do not support MFA and develop a plan to either upgrade so these systems support MFA or migrate to new systems that support MFA. MFA support to business applications can often be added through integration with enterprise identity and single sign-on (SSO) systems. If this is not directly possible, there is technology available to integrate a wide variety of legacy system types with modern MFA and SSO. CISA recommends escalating any risks of any system that does not support MFA to the organization's senior leadership team.

## PHISHING-RESISTANT MFA IMPLEMENTATIONS

### FIDO/WebAuthn Authentication

The only widely available phishing-resistant authentication is FIDO/WebAuthn authentication. The FIDO Alliance originally developed the WebAuthn protocol as part of FIDO2 standards and is now published by the World Wide Web Consortium (W3C). WebAuthn support is included in major browsers, operating systems, and smart phones. WebAuthn works with the related FIDO2 standard to provide a phishing-resistant authenticator. WebAuthn authenticators can either be:

- Separate physical tokens (called "roaming" authenticators) connected to a device via USB or near-field comms (NFC), or.
- Embedded into laptops or mobile devices as "platform" authenticators.

In addition to being "something that you have," FIDO authentication can incorporate various other types of factors, such as biometrics or PIN codes. FIDO2-compliant tokens are available from a variety of vendors.

### PKI-based MFA

A less widely available form of phishing-resistant MFA is tied to an enterprise's PKI. PKI-based MFA comes in a variety of forms; a well-known form of PKI-based MFA is the smart cards that government agencies use to authenticate users to their computers. PKI-based MFA provides strong security and is sensible for large and complex organizations.

However, successfully deploying PKI-based MFA requires highly mature identity management practices. It is also not as widely supported by commonly used services and infrastructure, especially in the absence of SSO technologies. In most PKI-based MFA deployments, a user's credentials are contained in a security chip on a smart card, and the card must be directly connected to a device for the user to log into the system (with the correct password or PIN). The U.S. government's personal identity verification (PIV) card and common access card (CAC) are examples of PKI-based MFA.

## AREAS OF FOCUS FOR IMPLEMENTING PHISHING-RESISTANT MFA

### Prioritizing Implementation Phases

CISA recommends an organization's IT leadership consider the following questions to help prioritize the migration to phishing-resistant MFA into logical phases:

- **What resources do I want to protect from compromise?** For example, cyber threat actors often target email systems, file servers, and remote access systems to gain access to an organization's data. They also try to compromise identity servers like Active Directory, which would allow them to create new accounts or take control of user accounts.
- **Which users are high-value targets?** While the compromise of any user account can create a serious security incident, every organization has a small number of user accounts that have additional access or privileges, which are especially valuable to cyber threat actors. For example, if a cyber threat actor can compromise the account of a system administrator, they may be able to access any system and any data in the organization. Other examples of high-value targets are attorneys—who may have e-discovery permissions to read email, including deleted email, of staff members—or HR staff, who may have access to personnel records.

### Common Issues and Paths Forward

When starting their deployment of phishing-resistant MFA, organizations run into common stumbling blocks. Common issues and possible paths forward include:

- **Some systems may not support phishing-resistant MFA.** Perhaps the product is no longer supported by the vendor, or the vendor has not yet prioritized the work to implement phishing-resistant MFA. Regardless, CISA encourages organizations to first focus on the services that do support phishing-resistant MFA, e.g., most hosted mail and SSO systems support FIDO; these systems are good starting points because the data is valuable, and the vendors likely support FIDO.
- **It may be difficult to deploy phishing-resistant MFA to all staff members at once**. For example, it may be impractical to train, enroll, and support all users at the same time or there may be other operational considerations that prevent the organization from rolling out phishing-resistant MFA to some groups in the first phase. Consider which groups might be appropriate for an initial phase, e.g., help desk and IT system administrators. Later phases can expand from there, incorporating lessons learned from the earlier phases.
- **There may be concerns that users will resist a migration to phishing-resistant MFA.** IT security leadership should present the risks associated with not having MFA—or with deploying or maintaining potentially vulnerable MFA—to the organization's top leadership for approval. Should the organization's senior leadership decide that the risk of not using phishing-resistant MFA is too great, they are best positioned to manage cultural and communications challenges to implementation.

## RESOURCES

- For more information on MFA, see CISA's MFA webpage, CISA's MFA factsheet, and CISA's Capacity Enhancement Guide: Implementing Strong Authentication.
- See the FIDO Alliance's User Authentication Specifications for information on FIDO2 authentication specifications: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and the Client to Authenticator Protocols (CTAP).

## DISCLAIMER

The United States Government through CISA of the Department of Homeland Security (DHS) does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise is provided for informational purposes and does not constitute or imply their endorsement, recommendation, or favoring by CISA or DHS.