What is Phish Proof MFA?

IDEE

Table of contents

Phish Proof MFA

Phish-proof multifactor authentication (MFA) is a multifactor authentication process that assures the user identity and authentication attributes cannot be intercepted, modified and/or subverted by an attacker using phishing techniques. It ensures that the complete user identity lifecycle including registration, identity proofing, authenticators establishment, authentication, recovery, re-identification, and account termination are immune to phishing attacks.

Phish-proof MFA unlike phishing-resistant MFA does not only prevent attackers from intercepting and tricking users into revealing access credentials, it also, assures that the chain of trust established at the stage of user identity proofing is transitive, cannot be broken and provable.

Phishing

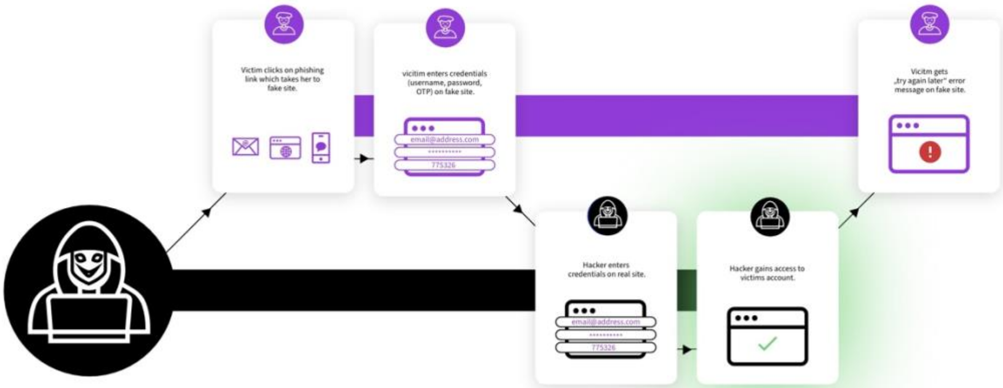
According to NIST phishing refers to an attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier or relying party and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier or relying party. The major component of phishing is “deception”. Attackers use deception tactics to convince the user into giving away personal sensitive information such as passwords. Unknowing to the victim, the revealed information is utilised by the attacker to access the victim’s account, monitor communications, carry out illegitimate transactions and can even take-over the account. This deception can happen in so many ways and via different channels. The typical method of phishing is via email, an attacker sends a link to a fake site to a target’s email (this is called spear phishing). This can also be done using SMS (smishing) and on social media platforms. An attacker can embed a link on a genuine website to redirect unsuspecting users to a fake site or even call a user on their phone to deceive them into granting access to their account (vishing). The one common denominator is the human element. As reported in the Verizon 2022 DBIR - 82% of all breaches were caused by the human element.

How phishing works

There are many methods used by attackers to phish their victims. The information targeted determines the method. Here we explain some of the methods.

Credential Phishing

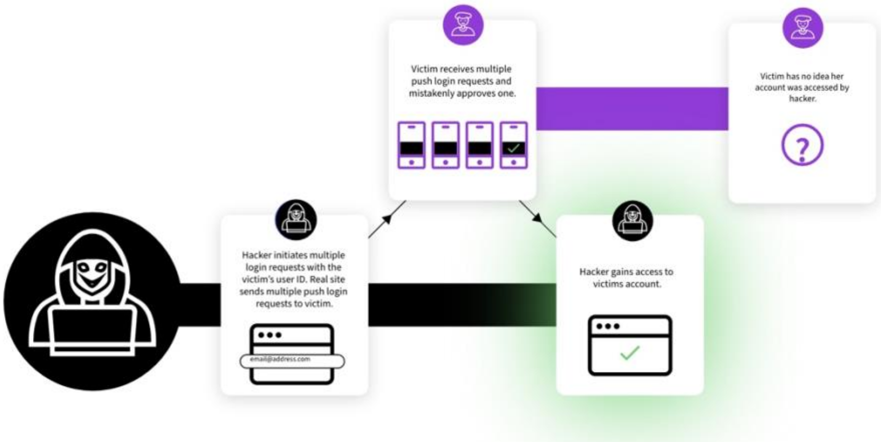
In credential phishing attacks, attackers disguised as trusted senders of email, SMS messages or legitimate websites to trick the victim into entering sensitive information. This is done by presenting fake login site or tricking the victim to click on an attachment or URL which sends the victim to a malicious imposter site. Stolen login credentials and sensitive information are used by cybercriminals to take over the victim’s accounts to impersonate the victim for financial and other fraudulent activities.


Victim clicks on phishing link which takes her to fake site.
vicitim enters credentials (username, password, OTP) on fake site.
email@address.com
****
775326
Hacker enters credentials on real site.
email@address.com
****
775326
Hacker gains access to victims account.
Vicitm gets „try again later“ error message on fake site.

The main target of an attacker in credential phishing is to obtain the victim’s credentials.

Prompt Bombing

Prompt bombing (MFA fatigue) relies on the victim to mistakenly grant the attacker access by approving just one push notification. With the victim's username such as an email address, an attacker can initiate login to the victim's account. Each login attempt sends a notification to the victim's phone. Out of annoyance or by mistake, the victim clicks on approve, and the attacker is in.

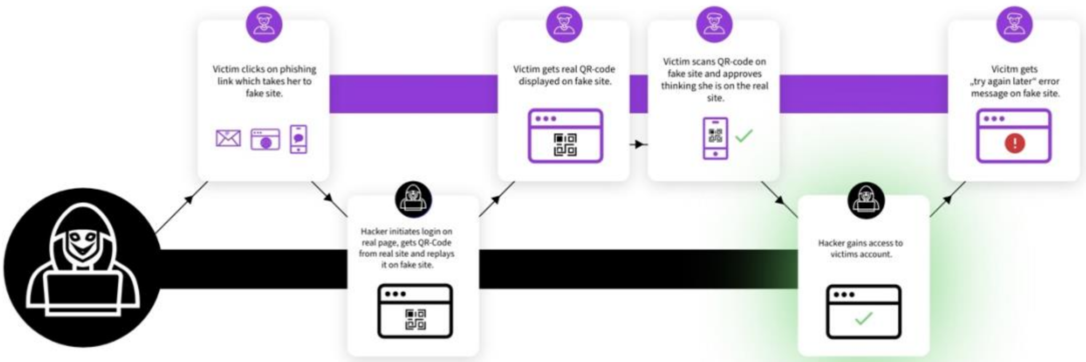

Hacker initiates multiple login requests with the victim's user ID. Real site sends multiple push login requests to victim.
email@address.com
Victim receives multiple push login requests and mistakenly approves one.
Hacker gains access to victims account.
Victim has no idea her account was accessed by hacker.
?

The attacker can then register their own authenticator device and lock the victim out of the account.

Here, the victim doesn't give credentials such as a password or OTP to the attacker. They still have their credentials intact, but they've granted access to the attacker.

QR Code Phishing

This is like prompt bombing in the sense that the attacker relies on the victim to mistakenly scan a QR code displayed on a fake website. This way the victim approves access and lets the attacker in.


Victim clicks on phishing link which takes her to fake site.
Hacker initiates login on real page, gets QR-Code from real site and replays it on fake site.
Victim gets real QR-code displayed on fake site.
Victim scans QR-code on fake site and approves thinking she is on the real site.
Hacker gains access to victims account.
Vicitm gets „try again later“ error message on fake site.

© 2022 IDEE | all rights reserved

The victim doesn’t give credentials such as password or OTP to the attacker. They still have their credentials intact, but they’ve granted access to the attacker. The attacker can then register their own authenticator device and lock the victim out of the account.

Consent Phishing

Consent phishing attacks exploit the use of OAuth 2.0 (a protocol that allows third-party apps to access a user’s account without the user’s interaction).

The goal of a consent phishing attack is to trick users into granting permissions (consent) to malicious attacker-owned applications. The user sign-in takes place genuinely via a trusted identity provider, after which the attacker asks the user to grant certain permissions to the malicious app. If the permission is granted, the service provider issues an access token to the malicious app. With this token, the malicious app can access the user’s account programmatically with the user’s knowledge. If the user has elevated privileges, the attacker can programmatically create new accounts, install ransomware, and backdoors for continual access to the user and/or organisation network.

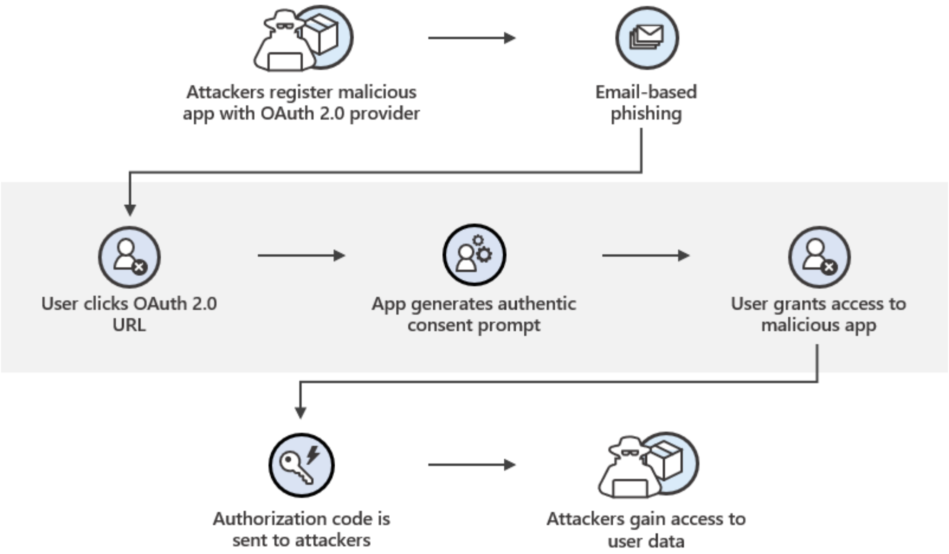

Attackers register malicious app with OAuth 2.0 provider
Email-based phishing
User clicks OAuth 2.0 URL
App generates authentic consent prompt
User grants access to malicious app
Authorization code is sent to attackers
Attackers gain access to user data

Diagram credit - Microsoft

Adversary-in-The-Middle (AiTM)

An Adversary-in-the-middle (AiTM) attack is a phishing technique whereby the adversary (attacker) deploys a proxy server between a target (user) and a website.

The proxy server intercepts the user's login credentials (username and password) and session cookie. Session cookies are used to prove the state of a user session so that the user doesn’t have to be authenticated at every new page they visit on the website.

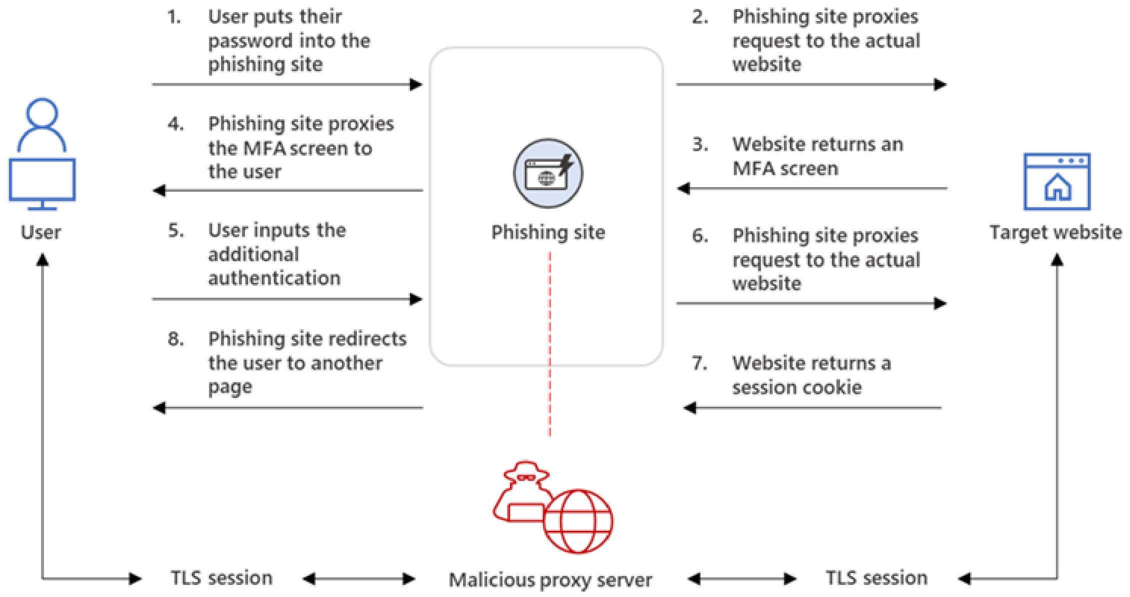

1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
4. Phishing site proxies the MFA screen to the user
3. Website returns an MFA screen
User
Phishing site
Target website
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
8. Phishing site redirects the user to another page
7. Website returns a session cookie
TLS session
Malicious proxy server
TLS session

Diagram credit: Microsoft

The intercepted session cookie is injected into the adversary's browser to access the user's account without the need for authentication even when MFA is enabled. This is because the session cookies prove to the website (web server) that the user has already been authenticated and has an ongoing session on the website. As a result, no further authentication is required.

The adversary can perform illegitimate transactions or steal sensitive data, takeover the compromised account by changing the authentication credentials (password and MFA), escalate its privileges in the organisation's infrastructure and install ransomware.

Why is phishing a big deal?

Phishing, unlike any other attack, leverages the "human element". Even if the technology and processes are securely designed, the people (human error) often give in to let attackers in. The human element drives breaches. Here are the facts about phishing:

1. The majority of all cyberattacks occur through stolen login credentials typically obtained through various forms of phishing attacks – NIST

2. All MFA processes using shared secrets are vulnerable to phishing attacks. Shared Secret authenticators include memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, one-time-passwords (OTP) and others - NIST

3. 82% of all breaches were caused by the human element - Verizon 2022 DBIR

4. Financial services is one of the most targeted sectors of phishing scams. The majority of the phishing attack campaigns (80.7%) use techniques that bypass 2FA solutions using one-time password tokens or push notifications. 42% of these attacks are associated with account takeover. - Enemy at the Gates: Analyzing Attacks on Financial Services by Akamai

5. 78% of Azure AD identities can be phished – "require only a username and password to authenticate" - Microsoft

6. 77% of intrusions are caused by three initial access vectors: phishing, exploitation of known software vulnerabilities and brute-force credential attacks. Phishing accounts for 37% of initial access. 70% of these incidents led to ransomware and business email compromise (BEC). - Palo alto networks' 2022 incident response report

7. 41% of business email compromise (BEC) involved Phishing - Verizon 2022 DBIR

8. Phishing is the costliest form of data breach, USD 4.91 million in breach cost - IBM

Phishing attacks are becoming more sophisticated making it much more difficult to defend. One of these sophisticated tactics is Adversary-in-The-Middle (AiTM) that bypasses MFA. As reported by the Microsoft 365 Defender Research Team, more than 10,000 organizations have been targeted by AiTM phishing campaigns since September 2021 using the Evilginx2 opensource phishing toolkit. US government in OMB M-22-09: stipulate that agencies "must use strong MFA throughout their enterprise" as follows "agency staff, contractors, and partners, phishing-resistant MFA is required. For public users, phishing-resistant MFA must be an option".

Recent phishing attacks

Here's a list of some of the recent phishing attacks.

Who	What	Why	When	Impact
Reddit	Employee's credentials were stolen	MFA vulnerable to credential phishing	2023	Attackers accessed "internal documents, code, and some internal business systems"
Dropbox	Employee's credentials were stolen	MFA vulnerable to credential phishing	2022	Attackers accessed "Dropbox's GitHub repository. 130 code repositories copied."
Uber	Employee's credentials were stolen by Lapsus$ ransomware group	MFA vulnerable to prompt bombing (MFA fatigue)	2022	Attackers had "full administrative access to Uber's cloud services…accessed the company's network and forced it to take several internal communications and engineering systems offline"
Microsoft	Employee's credentials were stolen by Lapsus$ ransomware group	MFA vulnerable to prompt bombing (MFA fatigue)	2022	Lapsus$ compromised Microsoft resulting in "limited access" to company systems
CISCO	Employee's credentials were stolen by the Yanluowang threat actors	MFA vulnerable to prompt bombing (MFA fatigue)	2022	The attacker gained access to "critical internal systems, such as those related to product development, code signing, etc"
Okta	Employee's credentials were stolen by Lapsus$ ransomware group	MFA vulnerable to prompt bombing (MFA fatigue)	2022	Lapsus$ accessed "an Okta internal administrative account… and about 2.5% Okta customers".
Twilio	Employee's credentials were stolen	MFA vulnerable to Smishing	2022	The attackers gained access to some of Twilio's internal systems

Multifactor Authentication

Multifactor Authentication (MFA) is an authentication mechanism that requires more than one distinct authentication factor. For an authentication to be considered multifactor, it must use more than one factor.

A factor (authenticator) is something the claimant (user) possesses and controls that is used to verify the user's identity. A factor can be something the user knows (such as memorized secrets), something the user has (such as a device), something the user is (biometric) or contextual. An authentication mechanism that requires just one of these factors is referred to as 'single factor authentication'. When at least two of these factors are required, it is called multifactor authentication (MFA).

Multifactor authenticator is an authenticator that provides more than one distinct authentication factor. For example, a cryptographic authentication device with an integrated biometric sensor that is required to activate the device. The cryptographic authentication device (such smartphone, computers, and security key with a secure cryptographic module) is what the user has (possession factor). Biometric is another factor, what the user is (inherence). When these two factors are achieved using a single device, the device is referred to as a multifactor authenticator.

As you can see from the above, multifactor authentication can be achieved using a multifactor authenticator or by combining single authenticators that provide different factors.

Below are some examples of authentication methods and the corresponding factors.

Authentication method	Factors	Classification	Examples
Password	Knowledge	Single authenticator	Manually entering a password to login to websites
Email link	Possession	Single authenticator	Clicking on an email link to login to websites
SMS code	Possession	Single authenticator	Manually entering an SMS code to login to websites
Password + SMS	Knowledge + Possession	Combination of single authenticators	Manually entering a password and SMS code to login to websites
Password + Email code/link	Knowledge + Possession	Combination of single authenticators	Manually entering a password and code to login to websites
Password + One-time password (soft/hard token)	Knowledge + Possession	Combination of single authenticators	Manually entering a password and OTP to login to websites
Push notification or QR code on a device + Biometric or PIN	Possession + Inherence or Knowledge	Multifactor authenticator	Using an app on a smartphone to approve a notification or scan QR code to login to a website
External cryptographic device + Biometric or PIN	Possession + Inherence or Knowledge	Multifactor authenticator	Using FIDO2 security keys with a PIN or biometric to login to websites
In-built cryptographic device + Biometric or PIN	Possession + Inherence or Knowledge	Multifactor authenticator	Using WebAuthN with a PIN or biometric to login to websites

One commonality is that a verifier (the service provider or an identity provider) must store something to be able to verify and validate a user identity at the point of access.

The key difference is what is stored by the verifier and how the factor is provided by the user to the verifier. Here lies the problem with almost all MFAs – they can be phished.

Phishable MFA

All MFA processes using shared secrets can be phished. This includes memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, QR code, one-time-passwords (OTP) and others. Any MFA that relies on the vigilance of the user to detect and prevent disclosure of authentication secrets and valid authenticator outputs to attackers is phishable.

To prevent (resist) phishing, an MFA needs to able to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system. Only two of the MFA methods listed in 0 above can resist phishing – FIDO2 and WebAuthN.

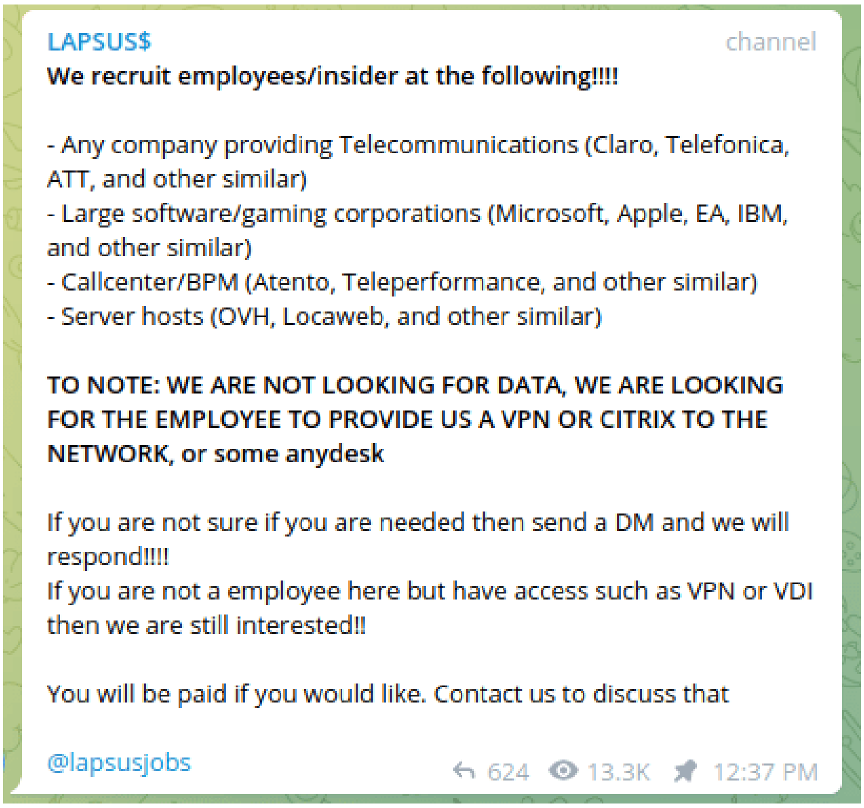
Phishing-resistant MFA uses asymmetric key cryptography for protection from phishing attacks. NIST SP 800-63-3 refer to them as cryptographic authenticators, this includes PIV/CAC cards, FIDO2 security keys and WebAuthN. FIDO2/WebAuthN are multifactor cryptographic authenticators that use a hardware cryptographic module to prove possession of an authentication secret through direct communication, via the endpoint, with a verifier. As a result, they are phishing-resistant **but not phish-proof.**

Is there a difference between phishing-resistant MFA and phish-proof MFA?

Yes, there’s a clear difference between phishing-resistant and phish-proof MFA. Phishing-resistant MFA is focused solely on the authentication process. Whereas phish-proof MFA focus on ensuring that the complete user identity lifecycle including registration, identity proofing, authenticators establishment, authentication, recovery, re-identification, and account termination are immune to phishing attacks. To simply put it, phishing-resistant is only a subset of phish-proof MFA.

According to NIST *“phishing resistant authenticators only address one focus of phishing attacks – the compromise and re-use of authenticators such as passwords and one-time* *passcodes. They do not mitigate phishing attempts that may have alternative goals such as installing malware or compromising personal information to be used elsewhere".*

As you can see, there's an inherent problem with phishing-resistant MFAs – identity proofing is decoupled from authenticator provisioning. The cryptographic device authenticators are added as an afterthought. This is made worst by the so-called best practice of having a "break-glass access and mandatory fallback authentication method" which is never the same as the primary authentication method. Attackers go for the weakiest link and in this case, would compromise the break-glass and/or the fallback authentication method to get into the kingdom. Phishing-resistant MFAs don't prevent the use of synthetic identity, identity proofing compromise, account takeover, insider threats and others.



LAPSUS$ channel

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

With initial access brokers (IAB) on the rise, phishing resistant MFAs cannot prevent malicious insiders from selling access to criminal gangs for financial returns. This is the modus operandi of the Lapsus$ ransomware group. They recruit insiders.

How can phishing be prevented?

The only sure way to prevent phishing is to use phish-proof MFA. Unlike phishing-resistant MFA that prevent attackers from intercepting and tricking users into revealing access credentials, phish-proof MFA in addition, assures that the chain of trust established at the stage of user identity proofing is transitive, cannot be broken and provable from start to the end of a user identity lifecycle.

Phish-proof MFA assures that the registration and identity proofing process cannot be compromised, that the established trust in the user identity at identity proofing is explicitly transited to the authenticator's establishment, and that the authenticators are based on a secure cryptographic authenticator device which is tamper-proof and tamper-resistant. It does not just stop there, phish-proof MFA ensures an end-to-end direct trust between the service provider (relying party) and the authenticator device. This trust cannot and must not be altered by intermediaries (such as identity providers). It ensures that the complete user identity lifecycle is immune to phishing, provable and cannot be subverted by a privilege insider.

With phish-proof MFA, detection, and prevention of disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system is only a subset of its attributes.

To put it simply, all phish-proof MFAs are phishing-resistant but phishing-resistant MFAs are not phish-proof.

Conclusion

1. Any MFA is better than no MFA.
2. Any MFA that relies on the vigilance of the user to detect and prevent disclosure of authentication secrets and valid authenticator outputs to attackers is phishable.
3. To be phishing-resistant, an MFA must:
    a. Prevent capturing of authentication data from the user
    b. Detect and prevent the use of authenticators at illegitimate websites
    c. Detect and prevent an adversary-in-the-middle from intercepting user authentication session cookies
    d. Eliminate the need of manual entry of authentication factors
    e. Prevent the replay of valid authentication outputs.
4. Phishing-resistant MFA only address one focus of phishing attacks – the compromise and re-use of authenticators such as passwords and one-time passcodes. They don't prevent the use of synthetic identity, identity proofing compromise, account takeover, insider threats and others.
5. Phishing-resistant MFAs are not phish-proof MFA.
6. Both resistant and phish-proof MFA use asymmetric key cryptography where the private key is used to digitally sign, and the public key is used to verify the signature. It provides authenticity and integrity protection and non-repudiation.
7. Phish-proof MFA doesn't only detect and prevent interception and usage of authenticators on fake website. It assures that the chain of trust established at the stage of user identity proofing is transitive, cannot be broken and provable from start to the end of a user identity lifecycle.

8. Phish-proof MFA ensures an end-to-end direct trust between the service provider (relying party) and the authenticator device. This trust cannot and must not be altered by intermediaries (such as identity providers). It ensures that the complete user identity lifecycle is immune to phishing, provable and cannot be subverted by a privilege insider.

The only sure way to prevent phishing is to use phish-proof MFA.

References:

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf
2. https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom
3. https://pages.nist.gov/800-63-3/sp800-63-3.html
4. https://www.microsoft.com/en-us/security/blog/2021/07/14/microsoft-delivers-comprehensive-solution-to-battle-rise-in-consent-phishing-emails/
5. https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf
6. Microsoft 365 Defender Research Team