Phishing-Resistant MFA: The Answer to the MFA Emergency

BEYOND IDENTITY

You never want to get that call. The one from the IT department letting you know your network has been attacked. But more companies are getting that call every day. So many, that it's becoming clear we are facing a cybersecurity emergency of epic proportions.

What's the emergency?

Old school MFA is being attacked and bypassed **at scale.** The first line of defense for many companies, considered a "standard of good practice" by insurance companies offering cyber insurance policies, is no longer effective. Companies and organizations are often required to implement MFA to qualify for new or ongoing cybersecurity policies. The problem is that relying on ineffective, phishable MFA is like posting a "keep out" sign and expecting bad actors to respect it.

The good news is that the pendulum is swinging. The US government has set a precedent for stronger security and government agencies are implementing changes at a rapid pace to meet stringent deadlines. **Phishing-resistant MFA is a necessity if you want to protect your organization's resources.**

Don't let traditional MFA fool you. The MFA nearly all organizations are using today is completely inadequate. Attacks, including those against Uber, Twilio, and Okta (0ktapus), show that bad actors are easily bypassing legacy MFA. In mid-2022 Microsoft reported a large-scale phishing campaign that allows the attacker to skip the authentication process even if the user has enabled MFA. Further attacks against Coinbase, SolarWinds, and Google, show the ineffectiveness of traditional MFA.

So why are companies using phishable MFA?

The insurance industry requires MFA as a minimum standard to help mitigate the effects of cyberattacks. Cyber insurance policies are becoming an absolute necessity for organizations. Unfortunately, the MFA those policies require isn't nearly enough protection when it comes to preventing attacks. It's just a matter of time before the insurance industry pivots to requiring modern, phishing-resistant MFA.

Leading the charge—US Government requires phishing-resistant MFA

The US government mandated in early 2021 that all agencies implement stronger identity and access management. President Biden's Executive Order on Improving Cybersecurity mandates "bold changes and significant investments" to the security infrastructure of government agencies. One of the primary requirements is the implementation of zero trust security.

On January 26, 2022, the Office of the Management and Budget (OMB) issued a memo setting the groundwork for the creation of zero trust architecture for federal agencies. The deadline for the objective for all government agencies and organizations that access government resources is the end of 2024.

The memo shows:

1. **All multi-factor authentication (MFA) is NOT created equal.** Agencies "must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."
2. **Phishable MFA factors should not be used.** "Phishing-resistant MFA" is mentioned over a dozen times in the memo.
3. **Zero trust requires solutions that provide cryptographic proof of user identity.** It's necessary to limit access and utilize continuous authentication. "Every request for access should be evaluated to determine whether it is appropriate, which requires the ability to continuously evaluate any active session."

The ripple effect of these new requirements will quickly spread to the public and private sectors, and the use of phishing-resistant MFA will become the new requirement whether specifically mandated in a regulation, or meeting the standard of due care in legal liability suits. These phishing-resistant requirements will also spread to other regulations (e.g., HIPAA, PCI, NYDFS, PSD2, SCA, CCPA).

What does this mean for you?

Now is the time to move toward the implementation of phishing-resistant MFA. Don't spend time and money on an outdated MFA you will need to rip and replace quickly. You must implement phishing-resistant MFA if you truly want to protect your resources.

If you are ready to protect your resources:

1. **Deploy phishing-resistant MFA today.** You'll need to implement MFA to renew or purchase a cyber insurance policy. Your policy may not yet require passwordless,

phishing-resistant MFA, but it is rapidly becoming the status quo. You won't want to rip and replace your phishable solution next year when the regulator and auditors take the government's lead and require passwordless and phishing-resistant MFA.

2. **Choose MFA that meets zero-trust requirements.** It is vital that you are ensuring that the endpoint device can be trusted before providing the user/device access. Your MFA must establish high trust in both the user and the device.

3. **Choose an MFA that is frictionless for end users.** You no longer have to make the security/usability tradeoff.

Beyond Identity can help you implement passwordless and phishing-resistant MFA that is also frictionless for your users. Schedule your demo today.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.