CISCO

Staying Vigilant Against MFA Attacks

What is an MFA fatigue attack?

Multi-factor authentication (MFA) fatigue attacks refer to types of cyberattacks that attempt to frustrate or overwhelm the user during the authentication process. When a user experiences friction upon trying to log in, they're more likely to look for a shortcut or workaround, which creates a major security risk.

Here's a quick look at factors that can lead to an MFA attack:



Lost or stolen credentials.

If attackers have a user's credentials, they can attempt to bypass multi-factor authentication methods. When a push notification is the second factor, the attacker may attempt what's called a "push bomb," the goal of which is to get the weary user to accept the push notifications – unknowingly giving access to the attacker.





Cybercriminals typically bypass MFA from unkown devices, so it's important to only allow authentication from trusted devices. A good defense against this is to implement policies that allow access to applications from devices that can be verified and managed.

Unauthorized MFA enrollment.

When someone gets hired at a company and receives their equipment, getting their devices enrolled in company systems is a critical step. However, if an attacker finds a vulnerability during that process, it creates a major security risk.





Inconsistent user experience.

If MFA processes in your organization are inconsistent across different systems or apps, users might find it confusing or difficult to navigate. The resulting frustration can lead to errors while logging in – making it easier for attackers to exploit the situation.

Noncompliance.

User training, security diligence, and reducing user friction are important in guarding against phishing in general. If an organization uses MFA for application access, it's important to monitor and enforce that policy. When users aren't compliant with that policy, it exposes the organization to potential attacks.



How can you stay protected from MFA fatigue attacks?

Make no mistake, attackers are always finding new ways to exploit, attack, and steal sensitive data. MFA fatigue attacks are just one of the ways attackers continue to evolve their methods. Therefore, to stay safe from these attacks, individuals and organizations alike must take every measure they can. It's no longer enough to rely on a single method alone – you need to develop a strategy and stick to it.

Here are some ways to stay protected:

Optimize the MFA process.

Implement strong MFA while preserving a good user experience. Using phishing resistant FIDO2 authentication mechanisms can be a gateway to achieve this.

Go passwordless.

• •



Simplify the MFA process even further. By negating the need for passwords, you'll not only increase security measures, but you'll greatly decrease the burden on IT and security teams in the process.

()

Risk-based authentication.

While challenging users with strong authentication factors improves security, it can also negatively affect the user experience. Use risk-based authentication techniques to assess the level of risk involved in each login attempt, such as where the login is occurring from.

Using device trust and trusted endpoints.

Keep a close eye on all user devices and monitor the network for anything that's out of compliance.

.

Gather feedback.

By conducting regular reviews of your security policy and MFA implementation, you'll have a finger on the pulse of what's working within your organization. It's a good idea to ask for user feedback and constantly evaluate the efficiency of your MFA policy.

Get the strongest protection against MFA attacks

Stay one step ahead of attackers with one access management solution: Cisco Duo.

With strong MFA protection and multi-layered defenses, Cisco Duo keeps bad actors at bay. It also uses risk-based evaluation methods, allowing users to indicate if they received a push notification they didn't initiate. This is one of the strongest and most effective ways to stay protected against MFA fatigue attacks.

Duo can also distinguish between unmanaged and managed endpoints to prevent attackers from attempting verification on their rogue devices using Duo Trusted Endpoints.

Additionally, Duo takes the headache out of remembering passwords with passwordless authentication. This feature is fully compliant with the FIDO2 (Fast Identity Online) industry standard and adds yet another layer of protection with phishing-resistant authentication.

What's more, Cisco Duo also features Verified Duo Push, which sends a PIN to the user's device. If an attacker sends that request from their own device, the user won't see it – ensuring your users stay much less susceptible to MFA fatigue attacks.

Try Cisco Duo

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 09/23