MFA Fatigue is Real!

Attackers will steal a username and password, then "push-bomb" the victim with MFA push notifications (phone pop-ups, app prompts, or codes). The goal is simple: annoy, confuse, or pressure the user into approving one request. One click is enough for account takeover.

If you didn't prompt it... Don't approve it!

Never Approve MFA You Didn't Initiate

MFA prompts should only appear immediately after you log in. If a request appears when you're not signing in, it means your password is compromised and is trying to get past MFA. Approving it hands them access instantly.

Report Repeated Push Notifications Immediately

Attackers often send dozens of MFA prompts in a short time hoping you'll approve one just to make them stop. This is a strong signal of an active attack and should be treated as a security incident, not an inconvenience.

Lock Your Account If Prompted Unexpectedly

When MFA prompts you without trying to log in, assume your password has been stolen. Locking or disabling your account stops the attack before MFA can be bypassed through continued prompts.

Change Your Password Right After MFA Spam

Obviously, if they are getting to the point where you are getting "push-bombed," your password needs changed. It is best practice to change your password immediately in order to thwart any chances of future attempts.

Use Number-Matching MFA When Possible

Modern MFA methods that require you to enter or match a number shown on the login screen are far more resistant to push-bombing. It is nearly impossible for them to guess the number through this method.

Treat MFA Abuse As A Security Incident

Many users dismiss MFA spam as an "IT issue" or "app glitch." But any delay can often allow attackers to succeed. MFA abuse means someone is actively trying to break in, so you need to broadcast awareness quickly.