Don't Get "Pushed" Into MFA Fatigue

A social engineering technique called **'MFA Fatigue'**, aka **'MFA push spam'**, is rising in popularity among hackers as it does not require malware or phishing infrastructure and has been found to be successful in attacks.

What is MFA Fatigue?
When an organization's multi-factor authentication is configured to use 'push' notifications, a prompt will be displayed on a mobile device when someone tries to log in with their credentials. These MFA push notifications ask the user to verify the login attempt and will show where the login is being attempted.

An MFA Fatigue attack is when a hacker runs a script that attempts to log in with stolen credentials over and over, causing what feels like an endless stream of MFA push requests to be sent to the account's owner's mobile device.

The goal is to keep this up, day and night, to break down the target's cybersecurity posture and inflict a sense of "fatigue" regarding these MFA prompts.

Ultimately, the targets get so overwhelmed that they accidentally click on the 'Approve' button or simply accept the MFA request to end the endless stream of notifications they were receiving on their phone.

What to do if you are a target of an MFA Fatigue/Spam attack
• Do not panic
• **DO NOT** approve the MFA request
• **DO NOT** talk to unknown people claiming to be from the bank
• Instead, **call your banker and explain that you think your account has been compromised and under attack**
• You should also **change the password for your account** to prevent the hacker from continuing to log in and generate further MFA push notifications. Once your password has been changed, the hacker will no longer be able to issue MFA spam.

Copy and paste this link into your browser to read the full article:
bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/