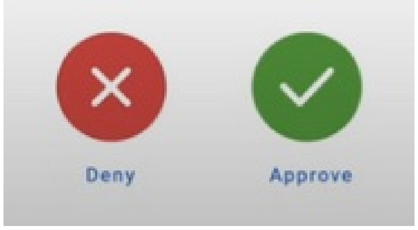
Complete Update

Are your employees equipped to defend against MFA fatigue? MFA fatigue refers to a type of cyber-attack where an attacker overwhelms a user with multiple multi-factor authentication (MFA) requests, hoping the user will approve one out of frustration. This tactic exploits the user's annoyance to gain unauthorized access to their accounts.

When an MFA fatigue attack happens, it means that an attacker has a valid username and password. The only thing preventing the attacker from entering your network is your user taking action to deny the MFA request.



Have your users been trained to know they should deny requests of this type? Do they know to contact the IT department immediately to report this and change their password? Would they know what to do after hours or over a weekend? You should consider requesting that employees have the phone numbers of the bank's Managed Service Provider (MSP) or IT staff programmed into their phones so they can report the attack and have their password changed or account locked. This will be important, especially if the attack occurs while on the golf course, at a child's event, or even in the middle of the night, when the user doesn't want to be distracted or just wants to be left alone.

-David McPhillips

Complete Compliance, Inc. | Email | Website | Newsletter | IT Newsletter |(402) 939-6715

The foregoing Compliance Update is for informational purposes only and does not constitute legal advice