Endeavour Foundation

Edition 6

Persistent MFA Prompts

Multi-factor authentication (MFA) can help you protect your online accounts by requiring that you approve login attempts before you can access the accounts. However, if you accidentally approve an MFA notification that you didn't request, cybercriminals may be able to access your accounts and personal information.

In a new scam, cybercriminals are annoying you into approving an MFA notification. If cybercriminals figure out your login credentials for an account, they can send you repeated MFA notifications. The cybercriminals hope that you will eventually approve a notification to stop the notifications from sending. Then, the cybercriminals can update the MFA settings in your account to send notifications to their device instead of your own. As a result, the cybercriminals can gain permanent access to your account and any personal information that's in the account.

Follow these tips to stay safe from MFA scams:

- Never approve an MFA notification that you didn't request.
- Create unique, strong passwords for each of your online accounts. If the cybercriminals can't figure out your password, they won't be able to scam you with MFA notifications.
- If you receive an MFA notification for an account that you aren't trying to log in to, immediately change your password for the account.

If in doubt, report the issue by raising a ticket at the #TeamPossible Support Hub or calling the ICT service desk on **1300 742 212.**

Stop, Look, and Think. Don't be fooled.