
# White Paper: Dealing with Phantom MFA Challenges in Microsoft 365

October 22, 2021

Jim Hill

**User Friendly Consulting, Inc.**

## Introduction:

In a recent article posted on the blog page of Schneier on Security, Roger Grimes wrote about his conversation with a Midwestern CEO whose company fell victim to a ransomware attack "to the tune of $10 million."[i] In this most timely and relevant blog post, Roger related how the attack chain began with a senior VP who had affirmed some ten different MFA push notifications for logins in which he was not directly involved. The article went on to say, "When the VP was asked why he approved logins for logins he was not actually doing, his response was, 'They (IT) told me that I needed to click on Approve when the message appeared!'" The VP's response highlights an emerging problem in every company that uses MFA, that of the phantom MFA challenge. If an employee approves a sign-in request for an application request in which they are not participating they are defeating the whole purpose of multi-factor authentication (MFA). The focus of this article is on Microsoft 365 but the principles apply to any environment.

Multi-factor authentication is a way of life for most employees. Whether it be a text message on their phone or a challenge request through their smart phone's authenticator app, we are all very used to responding to these things several times a day. Technical employees in our company can be asked to respond to MFA challenges every day from a long list of sources including the Microsoft Authenticator app on their smart phone, a challenge from the Zoho OneAuth app on their smart phone, a text message containing a confirmation code, and email containing a code, an automated phone call, a challenge from the Duo Mobile on their smart phone, or one of the many other methods used by our customers. Thankfully, finance and other businesspeople in our company are subject to a smaller subset of these methods.

## How the Phantom MFA Scenario Plays Out:

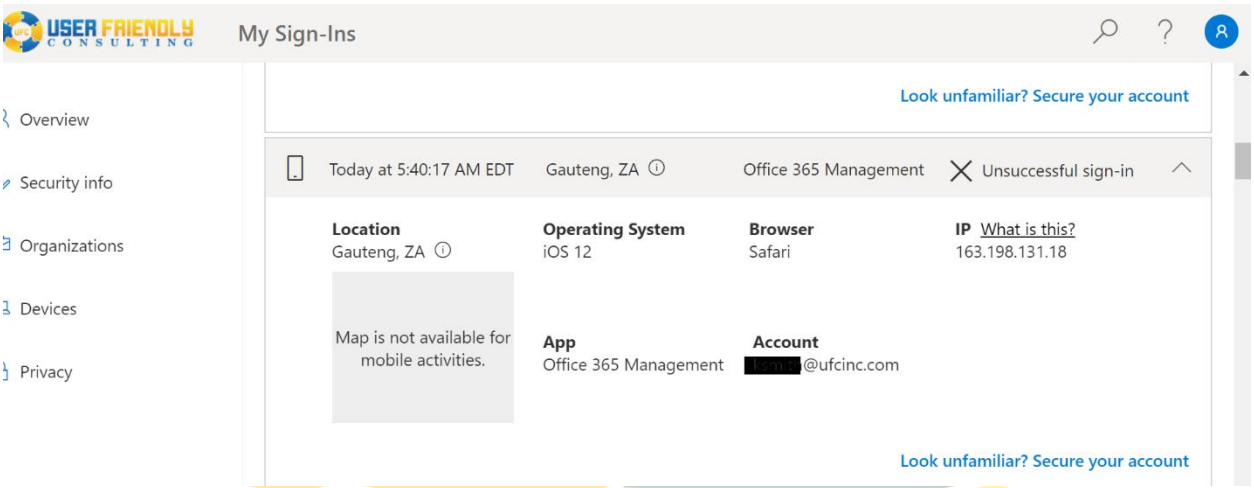
This is how a typical phantom MFA challenge scenario plays out from the perspective of real-life scenario that recently occurred in our company.

One afternoon I received a Teams chat from a senior level finance employee regarding an MFA challenge that they were receiving through their Microsoft Authenticator app on their smart phone. They had received a phantom MFA request as they were not aware of any application into which they were trying to access. Microsoft 365 users are very familiar with MFA requests which look something like this:


These MFA challenge push requests are really quite useless unless the user is immediately trying to log into a certain application and is expecting the request. Otherwise, they have no idea what application is trying to log in and any other details about the request.

After not responding to the request the employee proceeded to check their sign-ins page as this employee is much savvier than some less experienced computer users. They knew to check their “My

Sign Ins" page in Microsoft 365: https://mysignins.microsoft.com/ (available for enterprise customers). They then sent me the following image in Teams showing this suspect sign-in attempt:




Much information can be gleaned from this page, including that the requesting app was the Office 365 Management app via an iPhone running the outdated iOS12. However, the best plan of action is for the Microsoft 365 administrator to immediately begin an investigation through Azure AD. According to Microsoft on their Azure Active Directory blog, an unsuccessful sign-in, as shown in the screenshot above, indicates one of two things depending upon whether session activity is indicated in the lower right-hand corner of the report.[ii] If the login was unsuccessful and there was no session activity then the hacker used the wrong password. Second, if session activity was indicated then the user got past the password entry with a correct password but failed the MFA challenge. In this case the session activity was missing as it would have been noted in the blank space just below the IP address. This meant that the hacker located in South Africa (country code ZA) didn't in fact have the proper password. Strangely though, the failed login request fired off an MFA challenge on this employee's Microsoft Authenticator app. [Note, I posted about this discrepancy on that same Microsoft blog here.] Had this not occurred I would perhaps not have caught the failed login attempt until a few days later when I received my weekly AdminDroid login failure report.

## Actions that Microsoft Administrators can Take to Resolve this Scenario:

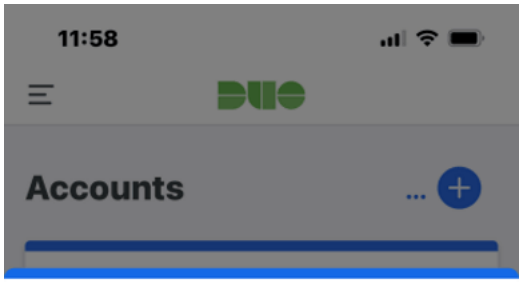
There are several actions that the Microsoft 365 administrator can take to prevent users from incorrectly affirming MFA challenges:

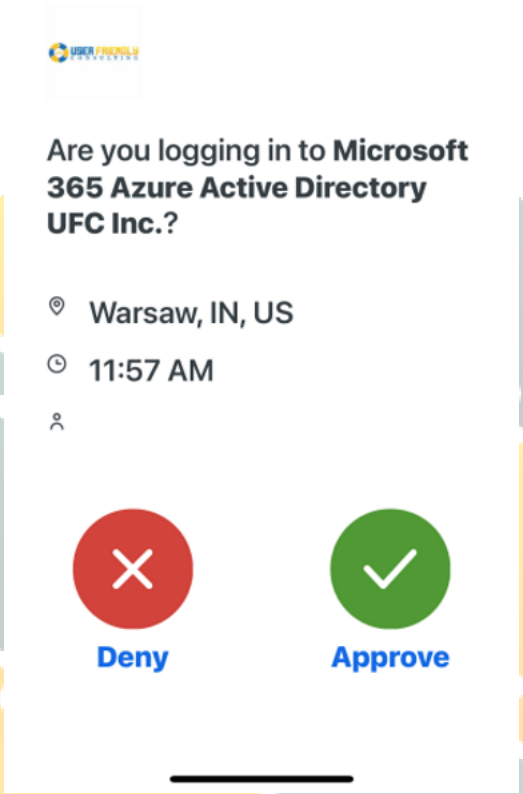
1. Consider replacing the Microsoft Authenticator app system with Duo MFA, at least for high risk employees and those with accounts under attack.
2. Train your users to deny and report phantom MFA challenge requests as well as how to read the My Sign-Ins report.

3. Implement robust conditional access (CA) policies in Azure AD so that any high-risk sign-in is blocked regardless of the MFA response.

**First**, the Microsoft 365 administrator should query their users and find out who, if anyone, has been experiencing phantom MFA requests. If these requests are denied in the Microsoft Authenticator, then the administrator will already have those reports. For this group of users, plus the ones who utilize a lot of devices (like me), and any other administrators, they should replace the Microsoft Authenticator app with the much more robust system provided by Duo. This cost-effective solution provides an immensely improved amount of information to help users to understand the MFA challenges that they receive on their phones.

The following is a typical MFA challenge presented by Duo for Microsoft 365:




If the user is expecting a challenge request, then it is very easy for them to approve it. Otherwise, they are provided with a host of information including an approximate location of the request, the time of the request, the username being authenticated, and the name of the requesting application.

Implementation of Duo is outside of the scope of this article; however, any Microsoft 365 administrator should be able to roll it out gradually to users using the excellent documentation provided by Duo. I would suggest that if you don't roll it out to the entire user base that you create a new security group and then place the affected users into the group. Implementation of the Duo MFA system is somewhat complicated, and it can be done in one of two ways. It can be rolled out first as a basic replacement for the Microsoft MFA app, or rolled out as a complete replacement in conjunction with a new CA policy in Azure as required by the integration.

**Second**, companies should educate every employee about the nature of the MFA challenge process along with the importance of denying phantom MFA challenges. Doing so would greatly reduce the amount of ransomware that is able to enter a company. Every user should know how to deny and report MFA challenge requests which they don't recognize, as well as how to use the My Sign-ins report.

**Third**, companies using Microsoft 365 should immediately adopt some basic CA polices in Azure AD. These polices should include at a minimum:

- Block all high-risk sign-ins.
- Block any sign-ins from foreign locations (such as the one from South Africa shown above).
- Block sign-ins from a list of risky IP addresses in any location.
- The policy required for the Duo MFA enterprise application.

Through the implementation of better MFA challenge systems, education of users, and incorporation of some basic CA polices, companies can greatly reduce the amount of incorrect MFA approvals. These actions alongside other common-sense things like disabling PowerShell for those employees who don't need it (see my post about this), better monitoring (for example through AdminDroid), and of course good offline backups could substantially reduce the amount of ransomware entering into companies.

---

[i] Schneier on Security https://www.schneier.com/blog/archives/2021/10/problems-with-multifactor-authentication.html cited 10/21/2021.

[ii] Microsoft, Azure Active Directory Blog, https://techcommunity.microsoft.com/t5/azure-active-directory-identity/users-can-now-check-their-sign-in-history-for-unusual-activity/ba-p/916066#:~:text=An%20Unsuccessful%20sign-in%2C%20which%20shows%20no%20session%20activity%2C,an%20attacker%20was%20trying%20to%20guess%20the%20password. Cited 10/21/2021.