Multi-Factor Authentication (MFA) News for TDS Portals

We are reaching out to inform you of a critical security enhancement that will soon be implemented across our services: Multi-Factor Authentication (MFA)

MFA is an additional security layer, requiring users to provide additional verification factors to access an account. This added measure significantly reduces the risk of unauthorized access, safeguarding both your personal information and our platform.

Here's why we believe MFA is essential:

1. **Enhanced Security**: MFA provides an additional layer of security beyond just a password, making it much harder for unauthorized individuals to access your account.
2. **Protection Against Phishing**: Even if a malicious actor obtains your password through phishing or other means, they would still need access to your secondary verification factor to gain entry.
3. **Compliance**: Many industry regulations and best practices recommend or require the use of MFA to protect sensitive data.

We understand that change can sometimes be challenging, but we are committed to ensuring that this transition is as smooth as possible for you. Here are the detailed instructions on how to set up MFA on your account, and our support team will be available to assist you every step of the way.

Activation of Multi-Factor Authentication (MFA)

Once Multi-Factor Authentication (MFA) is activated in the Portal, both internal and external users will receive an email notification with the subject: 'Multi-factor Authentication (MFA) was turned on for your account'.

Guidance for Setting Up MFA in TDS Portal

Upon accessing the TDS Portal, users will be directed to a setup page titled 'Mobile Authenticator Setup'.

Instructions:

1. **For Users with Authenticator App Installed:** If you've already installed the Authenticator app, in adherence to the **Tietoevry recommendation for Microsoft Authenticator**, adding a new profile is straightforward.
2. **Flexibility for External Users:** External users have the flexibility to utilize any Authenticator app they are currently using or install a new one from either the App Store or Google Play Store.
3. **Review Instructions:** You can also review detailed instructions in our documentation: Multi-factor authentication

Step-by-Step Guide:

- Open your Authenticator app on your mobile device or workstation (desktop).
- Tap 'Add Account' and select 'Work or school account'.
- Scan the Barcode: On the setup page, open the Authenticator app and scan the provided barcode. This action links the app to your account for multifactor authentication (MFA).
- Enter the One-Time Code: After scanning the barcode, the Authenticator app will generate a one-time code. Enter this code into the designated field on the setup page.
    - Note: If you have additional Authenticator profiles, please assign a name to the Device Name field: tds
- Complete Setup: Once the code is entered, click "Submit" to finalize the setup process. This ensures that MFA is successfully configured for your account.

blocked URL

If you are not able to use the Mobile Authenticator, use **the Authenticator Extension to your browsers.**

Please be aware that MFA does not impact TDS Service Accounts.

Users who have already enabled Multi-Factor Authentication (MFA) for their profile or workspace in the TDS Portal do not need to take any additional actions.

Schedule:

- PUB (https://pub.tds.tieto.com) (8th April 2024)
- INT (https://int.tds.tieto.com) **(29th April 2024)**
- FIN (https://fin.tds.tieto.com) **(29th April 2024)**

If you have any questions or concerns, please don't hesitate to reach out to our support team at **TDS Support Portal** or **TDS Mail Support**

Thank you for continuing to place your trust in our platform.

Warm regards,

TDS Team