USER

MUBEEN GUL MALIK

**DEP Task 2**

**Task 2**

**1.Objective:**Increase account security by implementing MFA.

**2.Description:**Set up multi-factor authentication (MFA) to add an extra layer of security to user accounts. Ensure MFA is user-friendly and effective.

**3.Key Steps:**

Selecting an MFA solution compatible with the system.

Configuring MFA settings and options.

Educating users on how to set up and use MFA.

Monitoring MFA adoption and addressing any issues.

Regularly updating and maintaining MFA configurations.

**Answer**

**Using: Microsoft Authenticator**

### 1. Selecting an MFA Solution Compatible with the System

* **Microsoft Authenticator** is highly compatible with various systems, especially if you’re using Microsoft products like Office 365, Azure, or Outlook. It's also widely supported for third-party applications that use MFA.

### 2. Configuring MFA Settings and Options

* **Adding Email Addresses:**
  + When setting up MFA with Microsoft Authenticator, you can configure multiple email addresses as backup or secondary methods for verification. This allows the system to send a 6-digit security code to these email addresses if needed.
* **Configuring SMS Authentication:**
  + If the option to send a code via SMS is selected but not available in Pakistan, you might need to disable or skip this option. Instead, rely on email codes or use the app's built-in code generator.
* **Choosing the Verification Method:**
  + When you log in, you may be prompted to choose between the configured email addresses to receive the 6-digit code. The user needs to select the correct email to receive the code for completing the authentication process.

### 3. Educating Users on How to Set Up and Use MFA

* **Step-by-Step Guidance:**
  + Provide clear instructions or tutorials on setting up Microsoft Authenticator. This should include how to add email addresses for recovery and how to generate and use the 6-digit code.
* **Highlighting Options:**
  + Make sure users know that if they are prompted to select an email for the code, they should choose the correct one from the options configured.
* **Alternative Methods:**
  + Since SMS may not work in Pakistan, educate users on alternative methods like using the app-generated code or email codes.

### 4. Monitoring MFA Adoption and Addressing Any Issues

* **Track MFA Usage:**
  + Monitor which users have successfully set up Microsoft Authenticator and if they encounter issues with receiving codes via email or the app.
* **Handling SMS Limitations:**
  + If users are attempting to use SMS but it’s not supported in their region, guide them towards using email or app-based codes. This can be handled through user support or FAQs.
* **Technical Support:**
  + Provide assistance to users who face difficulties in setting up or using MFA, especially regarding the 6-digit codes sent via email.

### 5. Regularly Updating and Maintaining MFA Configurations

* **Review Configurations:**
  + Regularly check the email addresses and other recovery options configured in the Microsoft Authenticator to ensure they are up to date.
* **Update Guidance:**
  + If Microsoft introduces new features or updates that impact how MFA works, inform users and update your educational materials accordingly.
* **Testing and Auditing:**
  + Periodically test the MFA setup, including the process of receiving and entering 6-digit codes, to ensure everything works smoothly.
  + 







