Test Case: Successful Login With Soft Token MFA (TOTP)

Steps:
1. Set up a Chrome driver and mock Mint.com login sequence for a user enrolled in TOTP/soft-token MFA.
2. Provide the user's email and password, set mfa_method=constants.MFA_VIA_SOFT_TOKEN, and mfa_token to a known TOT
3. Ensure oathtool.generate_otp(mfa_token) provides the correct current 6-digit code, either via mocking time or using a standard
4. Proceed with sign_in. Let it automatically submit the generated code at the MFA prompt.
5. Confirm that login is successful and returns a status_message (account sync complete, or equivalent).

Expected:
- No user input required (mfa_input_callback is None)
- Soft-token flow is used and the generated code passes MFA
- Account is accessed and sign_in completes

---Extra Details---
Filename: signIn.py
Description: Tests the integration of soft-token (TOTP) MFA for users, including automatic code generation and submission using
Score: 97%
Alignment: 92%
Validation Notes: Validates oathtool and MFA automation for TOTP and checks a major login flow that does not require email or S