New MFA Requirements for Accessing Research.gov

Cory Crew - 2024-10-29 - Comments (0) - Security

The Office of Information Technology (OIT) has recently been made aware of a late-breaking change that will affect the use of U.S. National Science Foundation (NSF) and Research.gov websites. **Effective October 27th, 2024, the U.S. National Science Foundation (NSF) is requiring Multi-Factor Authentication (MFA) for access to Research.gov.** With the growing number of cyber threats, the NSF has deemed traditional password-only security as no longer sufficient. **In order to access Research.gov after October 27th, you will need to use a Login.gov account bolstered with a 1Password Passkey** - a "phish-resistant" form of MFA. Brown University's usual MFA solution, Duo, does not currently meet this requirement, making 1Password Passkeys necessary for access to Research.gov.
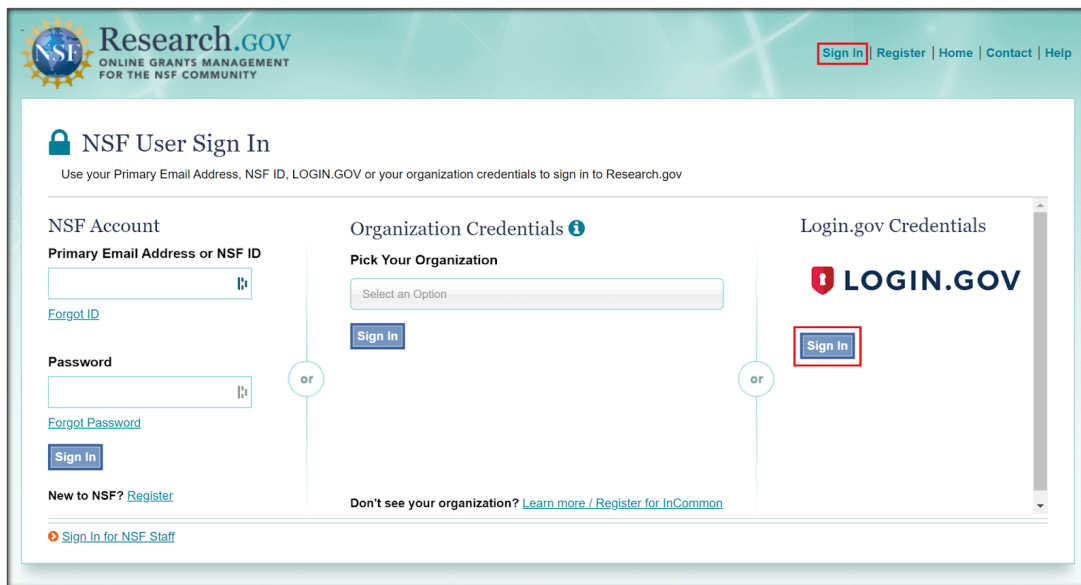
Login.gov has become a standard among government agencies, and we expect more federal services to adopt it as a primary access method in the future. 1Password is Brown's newly implemented password management tool, which securely stores and auto-fills credentials while supporting the latest MFA standards. Using a 1Password Passkey paired with Login.gov credentials will satisfy Research.gov's new login requirements. Please note that October 27th is not a deadline but the date when this change takes effect. You will be prompted to transition to this new login method upon your first login after October 27th at 10:00 AM Eastern Time.

A detailed tutorial on creating Login.gov credentials, setting up your 1Password Passkey, and accessing Research.gov, is outlined below. **We strongly recommend you set up and familiarize yourself with 1Password in advance of beginning the process outlined below. The process outlined below *requires* the 1Password browser extension, which can be download here.**

As a reminder, we strongly advise keeping Brown and personal credentials separate. This applies to Login.gov, 1Password, and all the services you use. Please ensure you use your Brown 1Password account for storing Brown-related credentials and access sites like Research.gov in your capacity as a Brown employee, using your Brown email address.

Creating new Login.gov credentials for accessing Research.gov

- Proceed to Research.gov, click "Sign In" in the upper right hand corner, and then click "Sign In" again under Login.gov.

- This will direct you to a Login.gov page where you can create your new MFA-compliant credentials. **Ensure you create this account using your brown.edu email account.**
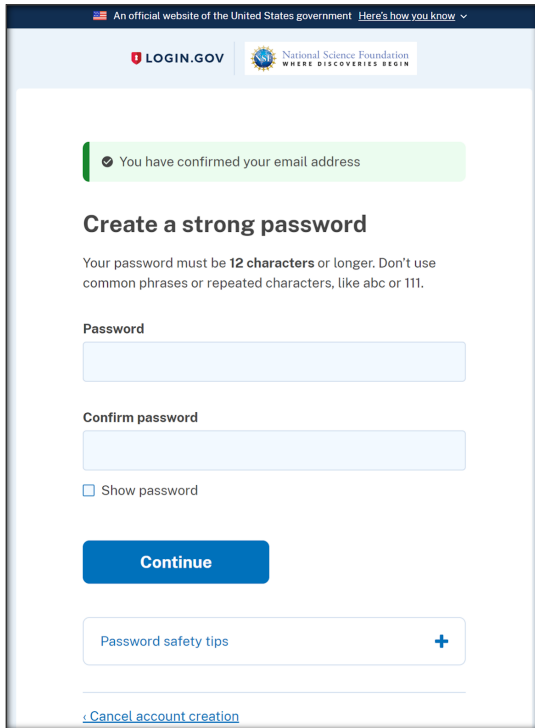
- After entering your email address, you will receive a confirmation email. Follow the link in this message to confirm your email address, establish your login credentials, and finalize creation of your account. Using 1Password will ensure your account

utilizes a strong and unique password.

- **If you do not already utilize 1Password for password management, now is an opportune time to begin doing so as 1Password is a requirement for later steps in this process, ensuring your MFA-compliant access to Research.gov is properly established. [Click here for an introduction to getting started with 1Password](#).**

- After finalizing your password, you will be presented with the option to add additional authentication options to further bolster the security of your account. Select the "Security key" option (i.e. 1Password Passkey), which is now *required* for accessing Research.gov.

- This will direct you to a page titled "Insert your security key". Enter a nickname for the security key, (we recommended calling it "1Password"), and then click "Set up security key".

- This will bring up a "Save passkey" popup from 1Password. Ensure your Brown email address is designated as the login, and click "Save".
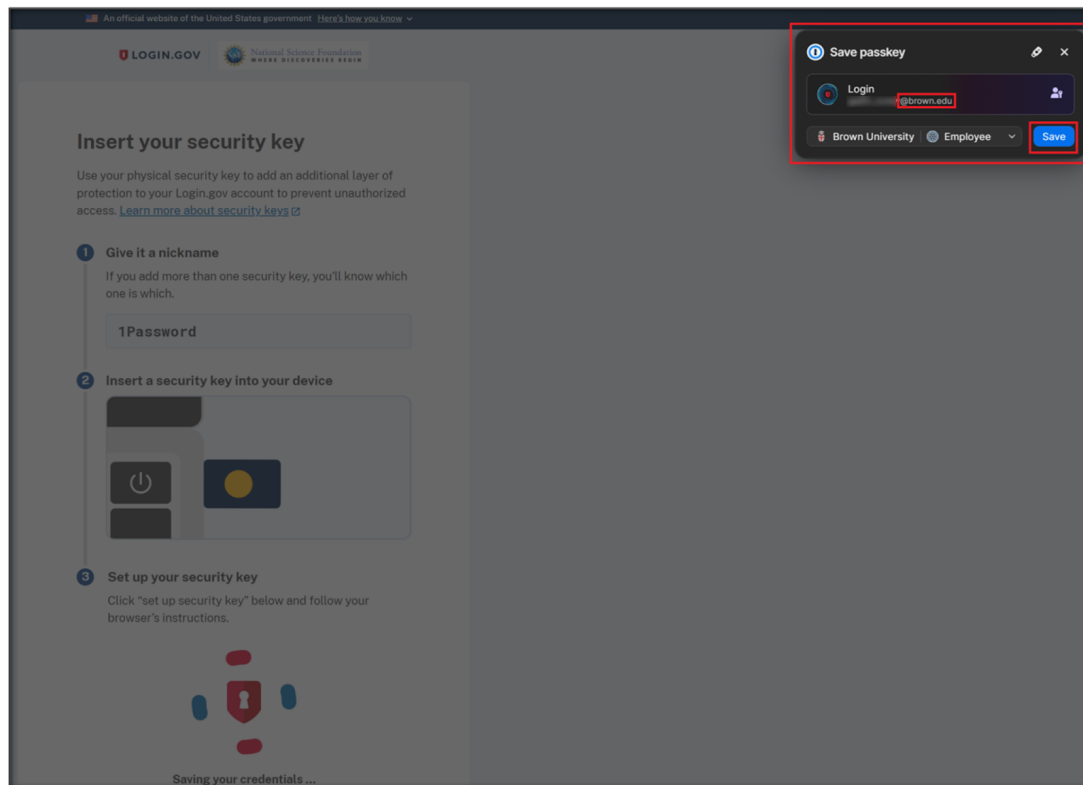
- You will see a confirmation message informing you that you have successfully added the 1Password Passkey to your Research.gov account. Click "Skip for now" to proceed.
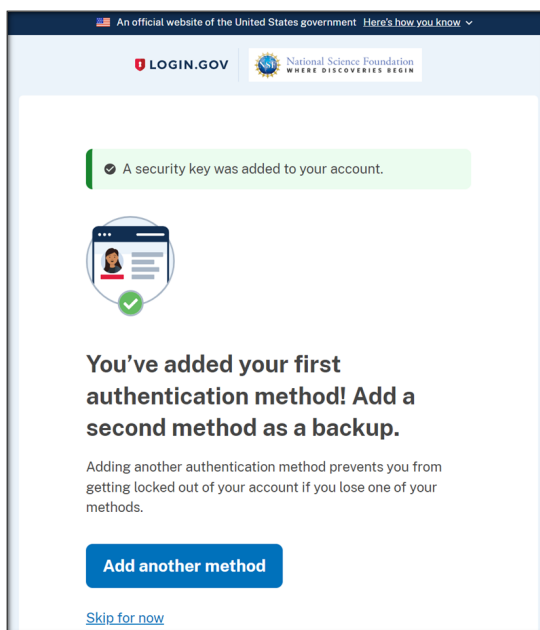
- Click "Agree and continue" to proceed back to Research.gov.

- Once directed back to Research.gov, you will have two options: link your existing NSF/Research.gov account to your new Login.gov account or create a new NSF/Research.gov account and link it with your Login.gov account. Anyone who has previously accessed Research.gov via an NSF account should link that existing account to their new Login.gov account.
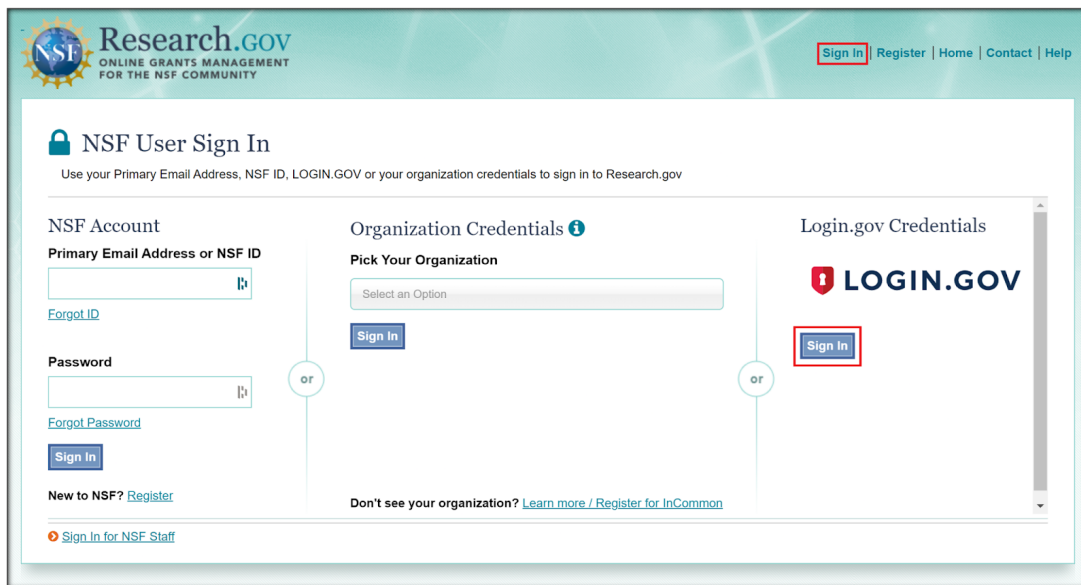

- You are now able to log in to Research.gov with your MFA-bolstered Login.gov credentials. To test this process, proceed to Research.gov, click "Sign In" in the upper right corner, and click "Sign In" again under Login.gov, as we did at the start of this guide.

- Enter your newly created Login.gov credentials and click "Sign in".
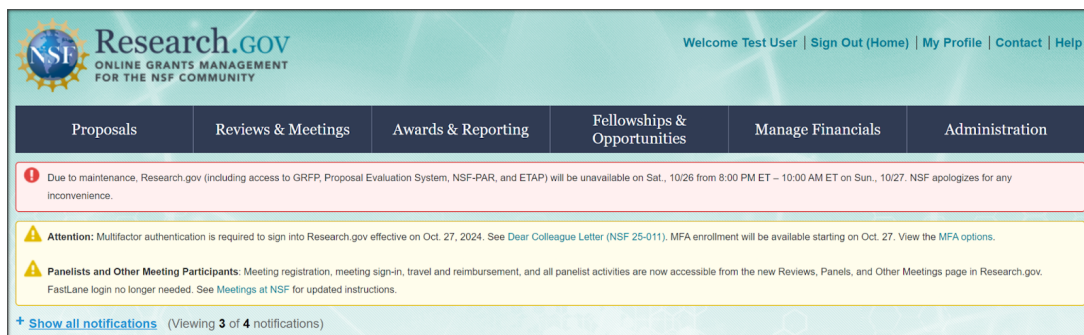

- On the following page, click "Use security key". 1Password will provide a popup, prompting you to complete your sign via the passkey you created in prior steps. Click "Sign in" to complete the process.
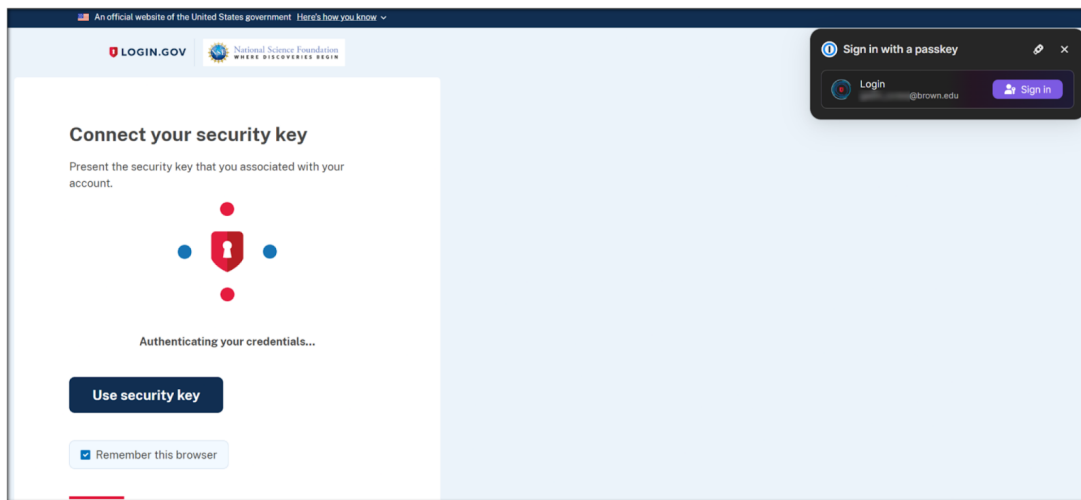
- Upon completion, you will be redirected back to Research.gov where you will be successfully logged in.

Additional Considerations

- We strongly recommend that community members transition to using Login.gov credentials instead of their existing NSF/Research.gov username and password. The Login.gov process, paired with a 1Password Passkey, meets NSF's new requirement for a phishing-resistant MFA method needed to access Research.gov. This transition will ensure uninterrupted access to NSF resources and streamline the authentication process. As outlined in the instructions above, you can link your existing NSF/Research.gov account to a new MFA-enabled Login.gov account.

- If you attempt to access Research.gov using Login.gov credentials without an enabled 1Password Passkey, you will receive the error message pictured below. In this case, select "Security key" as outlined in the steps above and proceed with creating a 1Password Passkey. This step will link the passkey to your Login.gov credentials, enabling secure access to Research.gov.

- Establishing a 1Password Passkey for use with your login.gov account will not remove or invalidate other MFA methods linked to your account. However, login.gov will automatically prioritize the most secure MFA option available. You may still use other MFA methods linked to your account that do not require a passkey, though these are considered less secure.