

Intuit – Two Factor Authentication

Intuit uses **multi-factor authentication** across all of their products, to protect your account and ensure only you have access to your data. As part of this verification, when you sign-in or when you make a change to your account information (such as email, password, user ID) you may be required to use a one-time confirmation code to complete the login process.



The following are answers to frequently asked questions about multi-factor authentication.

Why do I have to verify my account when signing in?

You can be assured that protecting your data and privacy is our #1 priority. You entrust us to protect sensitive data and we take that seriously. Our customers' privacy and security is job one. Multi-factor authentication is a common security practice for financial services and sensitive web accessible products. In order to keep your account secure, this feature cannot be disabled.

We always recommend that customers take precautions to protect their identity. It is important that users not only create strong passwords, but more important is not using the same password for all your accounts.

Security is a shared responsibility. Even with multi-factor authentication in place, users can help fight fraud by trying to make sure to:

- Do **not** use the same password for your Intuit products that you use for any other online product.
- Use unique information-not basic information that can easily be found online.
- When you receive email notifications, do **not** click on suspicious links. Instead, cut and paste the URL link directly into your browser.

What options do I have to verify my account?

- Phone – You can choose to receive your code via text message (Recommended Option)
- Email – You can choose to receive your code via email.

The ICB team notes that Intuit supports Authy and Google Authenticator in addition to standard email and SMS