Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security measure that will help verify your donors' identity and safeguard their payment details. This security feature is automatically enabled on all GiveSmart Fundraise payment forms when the credit card payment option is selected. There are no steps or settings to configure.

NOTE: PayPal, Venmo, and Digital Wallet payment options (such as Apple Pay and Google Pay) have their own integrated authentication methods, which allow them to bypass MFA. This makes them a suitable alternative for donors experiencing issues receiving their code or other challenges.

Click here to learn more about the different payment options available through your forms.

User Experience

Once a donor clicks the Submit Payment button at the bottom of a payment form, they will receive a prompt that a 6 digit code has been sent to the email entered on the form.

NOTE: The Email Address is a required field on payment forms, so all donors will need to enter an email address before reaching the payment step.

Once the code is entered, the donor will press the Enter button to be taken to the **confirmation page**.

The Importance of MFA for You and Your Donors

With a commitment to balancing ease of use with the highest level of security our customers and donors expect, a new Multi-Factor Authentication (MFA) security measure is enabled. This next level of protection will enforce even more security for your donors' identity and safeguard their personal information when completing payments on the GiveSmart platform.

What This Means for You
Multi-Factor Authentication (MFA) will be enabled on all existing and future payment forms in your Fundraise account. No additional action is needed on your part.

What This Means for Your Donors

When completing payments on Fundraise forms, donors will be prompted to verify their identity through a one-time code sent to their email. At this time, SMS authentication is not available and will be included as an option at a later date.

FAQs

What does the verification code email look like?

- The verification code email will be sent from noreply@givesmart.com, and will contain the following information.

Is the MFA verification code needed for non-payment forms?

- No, forms that do not include purchases, will not need a verification code.
- This includes: surveys, membership, volunteer sign-up and more.

Do I need a MFA verification code for a $0 purchase?

- Yes, if you are using a form element that includes a 'Price' field, even if the price is set to $0 then the multi-factor authentication workflow with the verification code will be part of the process to completing the form.

If paying with a digital wallet, is MFA necessary?

- No, MFA is not necessary when paying with a digital wallet payment option. This makes them a suitable alternative for donors experiencing issues receiving their code or other challenges.
- This includes **Apple Pay**, **Google Pay**, **PayPal** & **Venmo**.
- **Click here** to learn more about the different payment options available through your forms.

Why is multi-factor authentication important?

- By enabling this additional step in the payment process, this protects your organization from fraudulent credit card attempts on your payment forms.
- To learn more about how card testing, **click here**.

The donor didn't receive the email, where should they look?

- The email will be received from no-reply@givesmart.com which might have been caught in their spam filter. Please instruct the donor to search their spam file before resending the message.

Is there an option to receive the MFA via SMS (text message)?

- At this time, SMS authentication is not available but will be included as an option at a later date in 2025.

Can a user resend a code if the code has expired?

- Yes, a user can simply click the Resend Code link located at the bottom of the verification popup.