Securing Your Account Access

Your Flipcause Account is the key to your donor data, transaction data, and your merchant accounts - it's just like your bank account but potentially with even more sensitive information, including that of your constituents. Just like you would with your bank accounts, you'll want to take every precaution to keep it secure. Here is a list of best practices and steps to take:

Password Security

1. Use a strong password for your account. A strong password means:
   - Long (15+ characters is ideal)
   - Unique (you don't use this anywhere else)

2. Now that all your passwords are long, unique, and impossible to remember (good!) please use a password manager to store all of your long, (Never write passwords down anywhere!)

3. Do not share your login with other users. You have unlimited free sub-admin accounts available to you on Flipcause, and you can set specific permissions for each one. Please create a new login for each Flipcause user (or have us do it for you !)
Two-Factor Authentication

In case your username and password do get into the wrong hands, enabling this adds another layer of security to ensure that the person entering your login credentials is really you. *Not sure why this additional step is important? Read here.*

1. Set up **two-factor authentication** for your account
2. Make sure **your sub-admins also have two-factor authentication enabled**

Administrator Privileges and Settings

Each of your sub-admin accounts can be configured to have different privileges and levels of access. You'll want to give each of the people logging in only as much access as they need to keep your account secure. For example, you may want to block access to adding or editing linked bank accounts from most, if not all, subadmins.

1. Learn about access levels and the privilege options and how to set them up
2. Set up **Privilege Profiles** for different user types (such as volunteers vs. development staff vs. financial access)
3. If needed, restrict access to your Flipcause account based on location and set up email alerts for when suspicious logins are attempted.

Combating Fraudulent Transactions

Your Flipcause account comes with a proprietary and regularly updated security system that already blocks over 99% of all fraudulent transactions. This is above and beyond what your typical merchant accounts will offer. Plus, since all organizations have different needs, we have advanced features to give you even more control if you need it.

1. **Monitoring Transactions**
You should be monitoring your incoming transactions daily (if not in real time) to make sure they look legitimate. You can do this quickly by reviewing all of the transaction notifications that are emailed to you to check for the following common signs of fraud:

- Clearly fake names and email addresses (that look like jibberish)
- Uncommonly small transaction amounts
- A sudden high volume of incoming transactions

2. **Payment Security Settings**

If your organization's forms become the target of an attack, you will often find that they originate from a specific country or continent, and one that you wouldn't expect to receive donations or payments from usually. You can permanently or temporarily block those countries from being able to process transactions.

3. **Reporting Fraudulent Transactions**

If you do have any transactions that come through that you are sure are fraud, you will want to report them right away so we can refund them in full and remove these fake records from your database.

4. **What happens if you do nothing?**

If fraudulent transactions go through without being caught right away, this puts your organization at risk to chargebacks and their accompanying fees from the real credit card holders once they find out their cards have been misused. This could add up to tens if not hundreds of dollars in fees to your organization, which we work very hard to help you avoid. If you have any questions or concerns, please don't hesitate to reach out to your Success Team - we're here for you!

---

**Identifying and Avoiding Phishing and Spoofing Scams**

Phishing and spoofing refers to the practice of imitating legitimate website addresses and content, email addresses and email content, and other branding such as logos and company name to seem like they are coming from your vendor. Common examples
include pretending to be your banking institution, the IRS, or Google. They may even present themselves as Flipcause.

Because it's easy for anyone to set up a similar-sounding email address and website name to a real company, this practice is common and impossible to prevent from occurring. The only thing that can be reliably done is learning how to spot these scams, and the good news is most of these fakes follow the same patterns and are incredibly easy to spot, once you know what to look for.

Always pay attention the URL in your browser and the URL inside the link. Flipcause pages always end in Flipcause.com. Flipcause sites will never ask you to download any software, plugins, or extensions.

**Signs you may have received a phishing email:**

1. **Unofficial "from" email address.** The first sign of a phishing email is a sender email that is similar to, but not the same as, the company's official email address. Fraudsters often sign up for free email accounts with company names in them (such as "flipcauseaccount@yahoo.com"). These email addresses are meant to fool you. Official email from Flipcause always comes from an "@flipcause.com" email address.

2. **Urgent action required.** Fraudsters often include urgent "calls to action" to try to get you to react immediately. Be wary of emails containing phrases like "your account will be closed," "your account has been compromised," or "urgent action required." The fraudster is taking advantage of your concern to trick you into providing confidential information.

3. **Generic greeting.** Fraudsters often send thousands of phishing emails at one time. They may have your email address, but they seldom have your name. Be skeptical of an email sent with a generic greeting such as "Dear Customer" or "Dear Member".

4. **Link to a fake web site.** To trick you into disclosing your username and password, fraudsters often include a link to a fake web site that looks like (sometimes exactly like) the sign-in page of a legitimate web site. Just because a site includes a company's logo or looks like the real page doesn't mean it is!
Logos and the appearance of legitimate web sites are easy to copy. In the email, look out for:

Links containing an official company name, but in the wrong location. For example: "http://flip_cause.com" and "http://flipcause.site.com/" are a fake address that don't go to real Flipcause sites. A real Flipcause web address will have only "flipcause.com" at the end (before any forward slashes /). For example: "http://help.flipcause.com" is a legitimate Flipcause address, as is it’s subpages such as "http://help.flipcause.com/help/security"

5. **Legitimate links mixed with fake links.** Fraudsters sometimes include authentic links in their spoof pages, such as to the genuine privacy policy and terms of service pages for the site they're mimicking. These authentic links are mixed in with links to a fake phishing web site in order to make the spoof site appear more realistic.

   - And look for these other indicators that an email might not be trustworthy:
     - Spelling errors and poor grammar.
     - Requests for personal information such as your password, Social Security number, or bank account or credit card number. Legitimate companies will never ask you to verify or provide confidential information in an unsolicited email.
     - Attachments (which might contain viruses or keystroke loggers, which record what you type).

**Signs you may be on a phishing site:**

1. **Check the web address.** Just because the address looks OK, don't assume you're on a legitimate site. Look in your browser’s URL bar for these signs that you may be on a phishing site:

   - Incorrect company name. Often the web address of a phishing site looks correct but actually contains a common misspelling of the company name or a character or symbol before or after the company name. Look for tricks such as substituting the number "1" for the letter "l" in a Web address (for

- "http://" at the start of the address on Flipcause sign-in pages. A legitimate Flipcause sign-in page address starts with "https://" — the letter "s" must be included.

- Incorrect domain. For example: "http://flip_cause.com" and "http://flipcause.site.com/" are a fake address that don't go to real Flipcause sites. A real Flipcause web address will have only "flipcause.com" at the end (before any forward slashes / ). For example: "http://help.flipcause.com" is a legitimate Flipcause address, as is it's subpages such as "http://help.flipcause.com/help/security"

2. **Be leery of pop-ups.** Be careful if you're sent to a website that immediately displays a pop-up window asking you to enter your username and password, or to download something.

3. **Give a fake password.** If you not sure if a site is authentic, don't use your real password to sign in. If you enter a fake password and appear to be signed in, you're likely on a phishing site. Do not enter any more information; close your browser. Keep in mind, though, that some phishing sites automatically display an error message regardless of the password you enter. So, just because your fake password is rejected, don't assume the site is legitimate.

4. **Be wary of other methods to identify a legitimate site.** Some methods used to indicate a safe site can't always be trusted. A small unbroken key or locked padlock at the left of the URL bar of your browser is not a reliable indicator of a legitimate website. Just because there's a key or lock and the security certificate looks authentic, don't assume the site is legitimate.

### Additional ways to stay secure

Check out our blog post for a full list of tips on cybersecurity to learn more about how to keep your organization secure.