Why Two-Factor Authentication Is a Must

The internet can be a scary place. Hackers keep getting more sophisticated in their methods to steal your credentials, but two-factor authentication continues to be our silver bullet. Microsoft found that 99% of hacker attempts are prevented by two-factor authentication.

When security breaches happen, hackers get access to thousands of password records for different accounts so your passwords can be revealed (you can even check here if your passwords have been hacked: https://haveibeenpwned.com/Passwords).

Even if you use best practices for password strength and security, this is no longer sufficient to keep your account secure.

With two-factor authentication enabled, it secures these accounts from being accessed by hackers even if they did get a hold of your login credentials. Also referred to as multi-factor authentication, 2FA, or MFA, we highly recommend setting this up for every account that you own that offers it.

How it works

The right to access an account or device no longer relies solely on the strength of a single password with multi-factor authentication (MFA). This easy to use security setting provides an added layer of protection for many types of accounts such as email, bank accounts and even social media profiles. It is also a simple security setting found on mobile phones and tablets. The technology requires at least two of the following types of identification methods before granting access to your information.

**Something you know** – static PINs, passwords, passphrases, answers to security questions.

**Something you have** – Smart card, token (e.g. MobilePass, Google Authenticator, Duo), mobile device (e.g. text containing a code), email address (e.g. email containing a code)

**Something you are** – Biometrics such as your fingerprint, retinal scan, facial recognition
What are the benefits?

1. **Improved security**: With MFA/2FA, there is the added layer of security with a unique one-time password that is generated every time you attempt to log in. To get that one-time password (token), you must possess the device or account that is receiving the token. This defends against the compromised passwords as the person trying to get into your account only has the password and not the device to gain access.

2. A good example of this is Flipcause's two-factor authentication process for admin accounts. You can set up your mobile phone as an additional authentication method via SMS or Google Authenticator. The two-step process is simple and helps ensure the security of your fundraising account, donor data, and hard-earned project funds.

3. **Reduced risk of data theft**: Hackers are not able to access your information if MFA is activated, therefore reducing the amount of information they can use to steal your identity. By enabling MFA on bank and credit accounts, anyone trying to impersonate you must verify your identity through two or more steps instead of a single password.

4. **Easy to use and cost-effective**: With today's technology, many accounts can easily enable MFA. From bank accounts, to airline and hotel rewards programs, MFA is either built into the company's website or can be set up using a 3rd party mobile app for little to no cost. MFA also does not require you to remember another obscure password that is difficult to remember, instead just have your mobile device with you.

Where to find it?

Multi-factor authentication can be found and turned on in Settings, Security, Privacy, or wherever you go to change your password for a mobile device. These popular sites, and many more, also offer multi-factor authentication:

- Flipcause
- Google
Click here for detailed instructions to help you set up multi-factor or two-factor authentication for the above list and many other sites. You can also visit TwoFactorAuth.org for a searchable more inclusive list of sites.