Member Up Security Guidelines

- All account information should be stored in a 1Password Teams account
  - Team members should only have access to accounts needed to do their job. For instance, someone managing content & social media does not need access to your hosting account information.
  - This isn't because of a lack of trust; rather, it's so that if any one individual's computer is compromised, the attackers have access to the least amount of information possible.
- **All passwords should be unique and automatically generated.** No words, no dates, etc. NO EXCEPTIONS. Here's an excellent article by Troy Hunt on this if you want to read more.
  - If passwords are reused, then any one service being hacked (Twitter, Facebook, Slack, etc.) means all your other accounts are instantly compromised as well.****
- Where possible, individual accounts should be used and invited to a Team account (e.g. Stripe).
  - This is so that account sharing is minimized. If accounts are shared, one person being hacked has a much larger impact than if no accounts are shared.
- Each team member's account in WordPress should have only the capabilities required for them to do their job, and no greater. For instance, if someone is only responsible for posting content, they do not need Administrator capabilities.
  - No shared accounts should be used – sharing WordPress accounts results in confusion about who did what, when. It also creates problems when someone leaves your company.
- All accounts should be *owned* by you the business owner, or at least associated with an email address controlled by you or your company (e.g. don't let a contractor set up your Twitter account under their email address).
  - This includes your Facebook page, Twitter account, and any other social media accounts.
  - This is so that when anyone leaves your company or an outside contractor stops working with you, there's no scramble to make sure you can still control your account - it's already in your control.
- Wherever possible, 2-factor authentication should be used (overview article). Basically, 2FA means that even if an attacker learns your password, they still can't access your account because a physical device is needed (usually your phone or a dedicated USB security key).
  - WordPress
  - Stripe
  - Facebook
  - Google accounts
  - etc.

This document was prepared by Travis Northcutt of Member Up.

Got any questions, or think something should be added? Shoot me an email: travis@memberup.co