Protect Your Social Media Accounts

Stephanie Obodda - 2023-04-28 - Comments (0) - General Security

We've put together this guide to help you keep your social media accounts safe.

Article Content

Email Accounts and Social Media

No matter what email address you use with your social media accounts (whether a personal or Brown social media account), we recommend that you:
(1) **Keep personal and Brown accounts separate**, i.e., use a personal email address for your own social media accounts, and only use your Brown email account for Brown-associated social media accounts,
(2) Have **unique passwords** for all of your accounts, and
(3) Turn on **two-step verification** for all accounts.

All of these precautions, especially two-step verification (also called multi-factor authentication or MFA) protects your other accounts and passwords from someone gaining control of your email and then resetting passwords for your other online accounts.

If your social media usage is part of your role at Brown, you may want to use your Brown email address when registering your social media account. This can provide additional security because if the email is compromised, OIT can more easily regain control of the email on your behalf.

If you are handling official social media on behalf of a department, you might want to use a general department address (for example, psychoceramics@brown.edu) to make it easier for another member of your department to continue using the account should you leave Brown. If you do not have a general address, you can request a "Google Shared Mailbox" from the IT Service Center.

If you would like to change the address associated with your social media account, see the following articles:

- Twitter: Updating Your Email Address
- Facebook: Settings > General > Contact (you can make an address your primary after adding it)
- LinkedIn: https://www.linkedin.com/help/linkedin/answer/60

Secure Your Phone

Make sure you secure your phone with a passcode, especially if you have social media apps installed. Otherwise, others can easily post to social media from your phone, whether it is someone with malicious intent or a curious toddler. For iPhones, we're recommending a six-character alphanumeric password (rather than numeric 4-character) because it's much more difficult to hack.

Related help articles:

- iOS: Use a passcode with your iPhone, iPad, or iPod touch
- Android: How to Secure Your Android Phone with a PIN, Password, or Pattern

Regularly Audit Access

- Did you share passwords to social media accounts with people who have left Brown? Change passwords periodically if they are shared.
- Is your Facebook page shared with people who have left Brown? This article describes where to find the list of people who have access: How do I manage roles for my Page?

Turn on Two-Step Verification on Social Media

Like Brown's Two-Step Verification, Twitter, Facebook, and LinkedIn offer an option to use a second factor of authentication such as a phone number or authentication app such as Duo Mobile. This is the best way to avoid account hacking.

Worried about inconvenience? Most websites only require this second factor on an unrecognized device or browser. If you normally access these accounts on one computer and one phone, it won't be a hassle.

Two-Step Verification for all of these websites requires you to have a cell phone number associated with your account.

If you are conducting social media on behalf of your department, a BIG consideration when turning on two-step is making sure that others are able to access the account should you leave Brown. Since it is tied to cell numbers, this can easily become an issue if you sign up with a personal cell number. When you first set up two-step, make sure to put the backup code in a place accessible by others in your department. Of course, you should also change the phone number on the account before you leave Brown.

Twitter

Turn on “Login Verification” by following the instructions in this article: Using login verification

Tips:

- Click “Generate Backup Code” to generate a one-time use code. Put this in a safe place accessible by others in your department who may need to access the Twitter account if you are unavailable or no longer at Brown.
- Click the “Setup a code generator app” button and scan the QR code with the Duo Mobile app you already use for Brown’s Two-Step Verification. This also lets you generate codes if your phone is offline / has no signal.

Facebook

Turn on “Login Approvals” by following the instructions in this article: How do I turn on login approvals?

Unlike Twitter, your Facebook page can be managed by more than one account. By turning on Login Approvals, you are just controlling access to your own account, which is used to manage the page. You do not need to share passwords or one-time use codes, you can just delegate access to other members of your department who are expected to update the page.

Tips:

- Click “Recovery Codes / Get Codes” to generate ten one-time use codes. No need to share these with others since they are related to your personal account, not the page.
- Click the text “third party app” in the Code Generator section and scan the QR code with the Duo Mobile app you already use for Brown’s Two-Step Verification. This also lets you generate codes if your phone is offline / has no signal.

LinkedIn

Turn on “Two-Step Verification” by following the instructions in this article: Turning Two-Step Verification On and Off

Tips:

- LinkedIn works by phone number / SMS code only. There are no backup codes and you can’t use an app like Duo to generate codes offline. However, LinkedIn does remember approved devices, so you could theoretically turn two-step off from one of those devices if you’re stuck without access to your phone number.