HIVE Helps

Social Media Security Guide

January 2023

READ ME!

In this guide, we'll cover how to secure your social media accounts using both a desktop internet browser and the mobile app for each social media platform. There are some common themes to securing every type of online account, including for social media. Read these to understand the "why", and then read on to understand the "how":

Secure your account with a strong password

A strong password is your first line of defense to protect your page. We recommend at least a 12 character password using upper and lowercase letters, numbers, and symbols. Your password should also be entirely unique from your other social media account passwords. If you're worried about remembering your password, or creating a stronger one, try using one of our recommended password managers (visit **www.hivesystems.io/password**).

Set up 2FA using an authenticator app

Two-Factor Authentication (2FA) is critical as a second line of defense for your social media account. If your password gets stolen, 2-factor authentication will keep hackers out of your accounts. The vast majority of social media accounts that get hacked are the result of not having 2-factor authentication turned on. However, some forms are more secure than others. While many sites offer a text message (SMS) based 2-factor authentication, the most secure way is to get an authenticator app that will provide you with refreshing 6-digit codes to use with your login.

Update your contact information

In the event that suspicious activity takes place on your page or you forget your password, you'll want to make sure that your email address, phone number, and other contact information is up to date so your account can be recovered.

Avoid suspicious requests and messages

If an account looks suspicious, it probably is. If an account's content has all been generated in the last day, it's likely a spam account. Also never respond to messages requesting personal information or money. Social media companies will never ask you for you password via email or direct message - so don't give it out!

About Hive Helps

Hive Systems provides non-profits pro bono support with our Hive Helps program. Great missions deserve great cybersecurity and we're here to help. Apply today online at **www.hivehelps.org**

facebook

NOTE: Your company's Facebook Page is managed and protected by your personal Facebook account - so make sure you, and any one else who manages your page, is secure!

Secure your Facebook account with a strong password

You can change your password by going to Facebook and clicking your profile picture at the top of the page and then **Settings & Privacy > Settings > Security and login** and click on **Change password**

You can change your password by going to Facebook, and clicking your profile picture at the top (or bottom) of the page and then **Settings & Privacy > Settings > Security and login** and click on **Change password**

Set up 2FA using an authenticator app

You can enable Two-Factor Authentication (2FA) by going to Facebook, and clicking your profile picture at the top of the page and then **Settings & Privacy > Settings > Security and login** and click on **Use two-factor authentication**

You can enable Two-Factor Authentication (2FA) by going to Facebook, and clicking your profile picture at the top (or bottom) of the page and then **Settings & Privacy > Settings > Security and login** and click on **Use two-factor authentication**

Create and monitor Page Roles

If you have a Facebook Page for your organization, you need to ensure the security of each personal Facebook Account that has access to it. Creating page roles enables you to control which accounts have specific permissions on your page. The 6 levels of roles have a variety of abilities and restrictions, with admin being the top. Be sure to only grant Page Roles to people you know and trust.

You can create and adjust Page Roles under **Page Settings > Page Roles**

Update your contact information

You can update your contact information by going to Facebook, and clicking your profile picture at the top of the page and then **Settings & Privacy > Settings > General > Contact** and click **Edit**

You can update your contact information by going to Facebook, and clicking your profile picture at the top (or bottom) of the page and then **Settings & Privacy > Settings > Personal Information**

facebook

Evaluate third-party apps and linked accounts

If you choose to use third-party helper apps to schedule your posts, enhance your uploads, or track data, you are adding risk to the security of your business account. Throughly research these apps and familiarize yourself with their Terms and Conditions before giving permission. Also, if you have linked multiple accounts, the security of those accounts is equally as important.

You can link an Instagram Business account to your Facebook Page to better secure both while also allowing you to easily share pictures and posts between them, manage comments, and manage direct messages.

- You can review your third-party permissions by going to Facebook and clicking your profile picture at the top of the page and then **Settings & Privacy > Settings > Security and login > Apps and Websites**
- You can review your third-party permissions by going to Facebook, and clicking your profile picture at the top (or bottom) of the page and then **Settings & Privacy > Settings > Security and login > Apps and Websites**

You can link your Facebook Page and Instagram Business account under **Page Settings > Instagram > Connect Account > Log in**

twitter

Secure your Twitter account with a strong password

You can change your password under **More > Settings and Support > Settings and privacy > Your Account > Change your password.**

You can change your password by clicking your profile picture at the top of the page and then **Settings and Support > Settings and privacy > Your Account > Change your password.**

Set up 2FA using an authenticator app

You can enable Two-Factor Authentication (2FA) under **More > Settings and Support > Settings and privacy > Security and account access > Security > Two-factor authentication** and check "Authentication app" and follow the prompts. Also under that same page, check "Password reset protect"

You can enable Two-Factor Authentication (2FA) by clicking your profile picture at the top of the page and then **Settings and Support > Settings and privacy > Security and account access > Security > Two-factor authentication** and turn on the toggle for "Authentication app" and follow the prompts. Also under that same page, turn on the toggle for "Password reset protect"

Evaluate third-party apps and linked accounts

If you choose to use third-party helper apps to schedule your posts, enhance your uploads, or track data, you are adding risk to the security of your business account. Throughly research these apps and familiarize yourself with their Terms and Conditions before giving permission. If you have linked multiple accounts, the security of those accounts is equally as important.

You can review your third-party permissions under **More > Settings and Support > Settings and privacy > Security and account access > Apps and sessions > Connected apps**

You can review your third-party permissions by clicking your profile picture at the top of the page and then **Settings and Support > Settings and privacy > Security and account access > Apps and sessions**

Update your contact information

You can update your contact information under **More > Settings and Support > Settings and privacy > Your Account > Account information**

You can update your contact information by clicking your profile picture at the top of the page and then **Settings and Support > Settings and privacy > Your Account > Account information**

Instagram

Secure your Instagram account with a strong password

You can change your password by clicking ☰ **More** in the bottom left corner and then **Settings > Change Password**

You can change your password by clicking your profile photo in the bottom right corner and then clicking ☰ in the top right and then **Settings > Security > Password**

Set up 2FA using an authenticator app

You can enable Two-Factor Authentication (2FA) by clicking ☰ **More** in the bottom left corner and then **Settings > Privacy and Security > Two-Factor Authentication**

You can enable Two-Factor Authentication (2FA) by clicking your profile photo in the bottom right corner and then clicking ☰ and then **Settings > Security > Two-factor authentication**

Evaluate third-party apps and linked accounts

If you choose to use third-party helper apps to schedule your posts, enhance your uploads, or track data, you are adding risk to the security of your business account. Throughly research these apps and familiarize yourself with their Terms and Conditions before giving permission. Also if you have linked multiple accounts, the security of those accounts is equally as important. For instructions on linking an Instagram Business Account with a Facebook Page, see Page 4 of this guide.

Update your contact information

You can update your contact information by clicking ☰ **More** in the bottom left corner and then **Settings > Edit Profile** and scrolling down to “Personal Information.”

You can update your contact information by clicking your profile photo in the bottom right corner and then clicking ☰ and then clicking **Account > Personal information**

NOTE: Your company's LinkedIn page is managed and protected by your personal LinkedIn account - so make sure you, and any one else who manages your page, is secure!

Secure your LinkedIn account with a strong password

You can change your password by clicking your profile picture with "Me" underneath it and clicking **Settings and Privacy > Sign in & Security > Change password**

You can change your password by clicking your profile picture in the top left corner and clicking **Settings > Sign in & Security > Change password**

Set up 2FA using an authenticator app

You can enable Two-Factor Authentication (2FA) by clicking your profile picture with "Me" underneath it and clicking **Settings and Privacy > Sign in & Security > Two-step verification**

You can enable Two-Factor Authentication (2FA) by clicking your profile picture in the top left corner and clicking **Settings > Sign in & Security > Two-step verification**

Create and manage Page Admins

If you have a LinkedIn Page for your organization, you need to ensure the security of each personal LinkedIn Account that has access to it. Creating page admins enables you to control which accounts have administrative permissions on your page. Be sure to only grant Page Admin status to people you know and trust.

You can create and adjust Page Admins by going to your organization's page, and clicking **Admin Tools > Manage Admins** under Settings.

Update your contact information

You can update your contact information by clicking your profile picture with "Me" underneath it and clicking **Settings and Privacy > Sign in & Security** and then clicking the arrow next to "Email addresses" or "Phone numbers"

You can update your contact information by clicking your profile picture in the top left corner and clicking **Settings > Sign in & Security** and then clicking the arrow next to "Email addresses" or "Phone numbers"

NOTE: If you use a YouTube "Brand Account" for your YouTube channel, it is managed and protected by your personal Google account - so make sure you, and any one else who manages your channel, is secure!

Secure your YouTube channel with a strong password

If you use a "Brand Account" for your YouTube channel:

- Your password for the account is your personal Google account password. If you need to check which account this is, go to YouTube and click on your profile picture in the top right corner and then click on **Manage your Google Account**
- Click on your profile picture in the topright corner again, and click on **Manage account**. Click **Manage Permissions** and you'll be prompted to enter your password for your personal Google account.
- Afterwards, you'll be taken back to the same screen, where you'll be able to click **Manage Permissions** again, only this time, you'll be shown anyone whose personal account is linked to you YouTube Brand account. So make sure each person has a strong password!

If you use a personal Google account for your YouTube channel, or are changing your linked personal account password:

- Go to YouTube and click on your profile picture in the top right corner (or sign in first if you need to) and then click on **Manage your Google Account**.
- Click on **Security** on the left side (or the top bar if you're on a phone), and then click on **Password** under the "Signing in to Google" section in the middle. You'll be prompted to enter your current password, and then you'll be able to set your new password.

Set up 2-Step Verification using an authenticator app

If you use a "Brand Account" for your YouTube channel:

- 2-Step Verification for the account is set through your personal Google account password.
- If you need to check which account this is, go to YouTube and click on your profile picture in the top right corner and then click on **Manage your Google Account**
- Click on your profile picture in the top right corner again, and click on **Manage account**. Click **Manage Permissions**, and you'll be prompted to enter your password for your personal Google account.
- Afterwards, you'll be taken back to the same screen, where you'll be able to click **Manage Permissions** again, only this time, you'll be shown anyone who has access to control your YouTube Brand account. So make sure each person has 2-Step Verification enabled

If you use a personal Google account for your YouTube channel, or are adding 2-Step Verification for your linked personal account:

- Go to YouTube and click on your profile picture in the top right corner (or sign in first if you need to) and then click on **Manage your Google Account**
- Click on **Security** on the left side (or the top bar if you're on a phone), and then click on **2-Step Verification** under the "Signing in to Google" section in the middle.
- Click on **Get Started** on the next page, and then you'll be prompted to enter your current password. You'll be asked to enter a telephone number, which Google will use to send you a text message.
- Click Next and Google will send you a text. Enter the six digits after the "G-" from the text in the box on the screen and click **Next**. Click **Turn On**

YouTube

While this is a good first step, you'll want to take advantage of the authenticator app we previously mentioned. You can also use the "Google Prompts" option if available:

- To do that, scroll down on the screen from the last step and click on **Set Up** under "Authenticator App."
- Select your phone type, and follow the instructions. Once you have the app installed on your phone, you'll use your phone's camera to take a picture of the bar code on the screen, then click **Next**. This will set up the rotating 6 digit codes on your phone.
- Google will ask you to enter this code to confirm you're set up correctly, and then click **Verify**
- Click **Done** and scroll back up on the page.
- Click the "Pencil" Icon next to the "Voice or text message" section and click **Remove Phone**

Update your contact information

- Go to YouTube and click on your profile picture in the topright corner and then click on **Manage your Google Account**
- Click on **Personal Info** on the left side (or the top bar if you're on a phone), and then under "Contact info," click on **Email**. Enter a "Recovery email". When done, click the arrow at the top next to "Email" to go back.
- Under "Contact info" again, click **Phone**, and enter a phone number.