A message from Aliro Marking to help make your Facebook Account more secure.

I am writing today because I am noticing a lot more successful (!) malicious hacking to Facebook & Instagram accounts and wanted to pass along some detailed instructions on how you can make your personal accounts safer so you don't lose control over your business pages.

To be clear, these instructions are for your ***personal accounts*** - but it does affect your business accounts on these platforms! Here's what's happening: Hackers get into your personal Facebook account & remove you as admin from your own business page in an attempt to extort you for money to get your business page back .... or you lose control of your business page altogether.

First, here are some security best practices for **Facebook:**

- Have a strong password that you don't use anywhere else. If you use the same password, change your Facebook (FB) password today. Be sure to include capital letters, lower case letters, numbers, & symbols.

- Appoint a trusted manager or business partner to be another admin on your FB page in case you get hacked & are removed as admin from your own business page. This way they can reinstate you. (If you're my client, you can rest assured that with me as an admin on your FB page, you'll be fine in this area for now. However, it's still probably a good idea to also add someone else from your business as an admin just for an added layer of protection.)

- Turn on 2-Factor authentication so you'll receive a text & verification code if someone does try to login as you. Without this verification code, the hackers can't access your page.

How to add 2-Factor Authentication to your Facebook (FB) account - Instructions:

1. Log into FB on a desktop computer

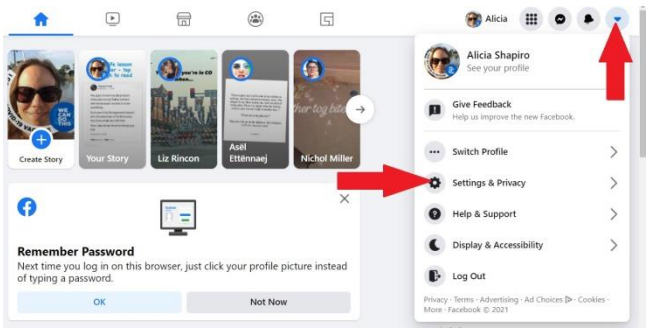
2. Click the drop down arrow in the far upper right corner, then click "Settings & Privacy" - see FB screenshot #1

3. Click on "Settings" - see FB screenshot #2

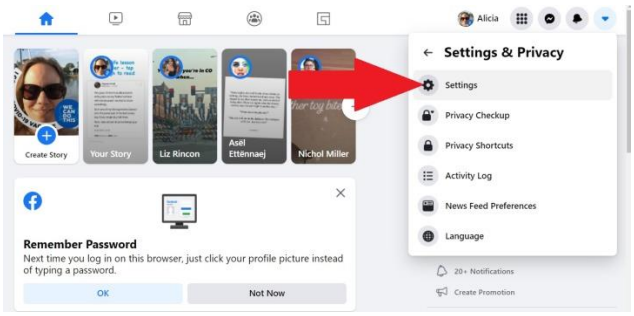
4. Click on "Security and Login" - see FB screenshot #3

- 5. On the Security and Login page, you'll see 3 things you need to do - see FB screenshot #4:
- a) Review the devices where you're logged into on Facebook to make sure these are YOUR devices. If they are your devices, you're fine - you have not been hacked. If you're unsure if these are your devices, click the "See More" in this section and at the bottom you'll see "Log Out Of All Sessions" - click that. This will log you out of Facebook everywhere - computer, phones, ipads, etc. (including any hackers that are currently logged in as you) - *but you'll need your current FB password to login/change your password, so before you log out, be sure you have your current FB password handy!*
- b) Change your FB password. Make it something that is entirely different from any other password you use, and be sure it's a strong password with capital letters, lower case letters, numbers, & special symbols.
- c) Turn on 2-Factor authentication & follow the onscreen prompts. This is extremely important because if someone tries to login as you/hack your account, you will get a text notification with a verification code to enter. If it is you logging back into your devices, simply enter the code & save your browser so it'll remember it's you next time. If you tell FB to save your browser you will not have to enter another code the next time you log in (however, you'll have to re-enter another code when you log in on your phone, but after that you'll be set ☺) Now, if you get another text like this, you'll know someone is trying to hack into your account & now they won't be able to because they won't be able to get this code.

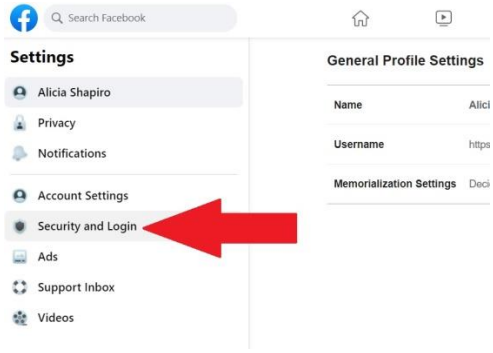
Facebook Steps



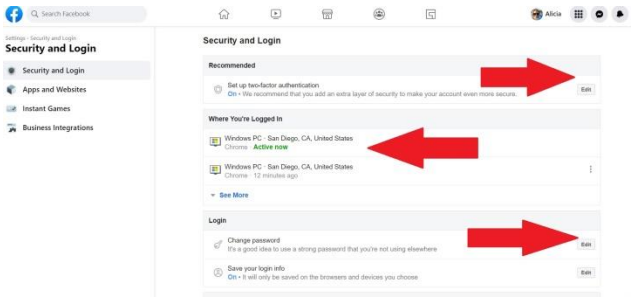
Step 1



Step 2



Step 3



Step 4

OCEAN BEACH MAINSTREET ASSOCIATION