SOCIAL NETWORK DOs & DON'Ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

MANAGING YOUR INSTAGRAM ACCOUNT

PROTECT YOUR INSTAGRAM INFORMATION
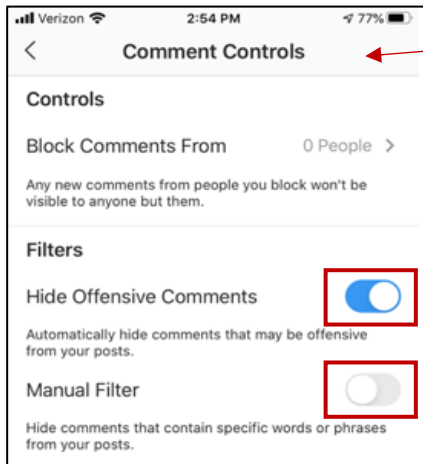
Edit your profile to display minimal personal information.

Touch the profile icon at the bottom of your screen.

Touch the menu icon (at the top of the screen) for options, select Settings, Privacy.
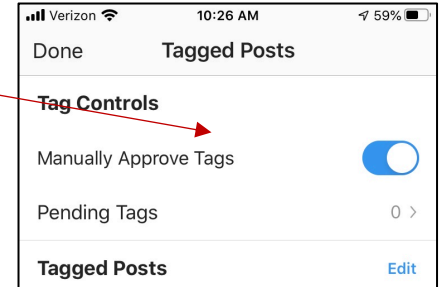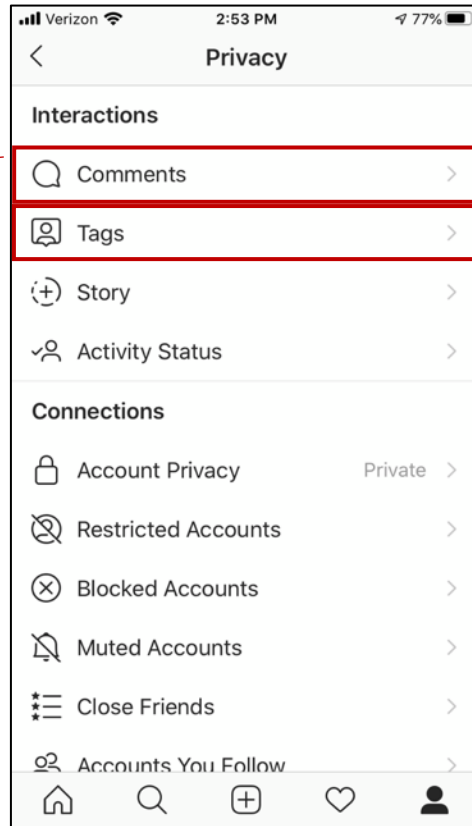
COMMENTS and TAGS:

At the Privacy menu review your settings.

Toggle on to hide offensive comments. Manual filter is also an option to hide specific words or phrases.

Toggle on to manually review any photos or videos before they are added to your profile by other users.

STORY, ACTIVITY STATUS and ACCOUNT PRIVACY:
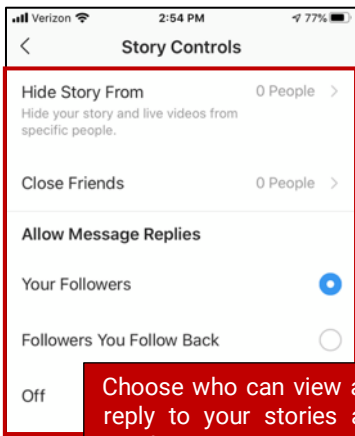
Choose who can view and reply to your stories and send you messages.
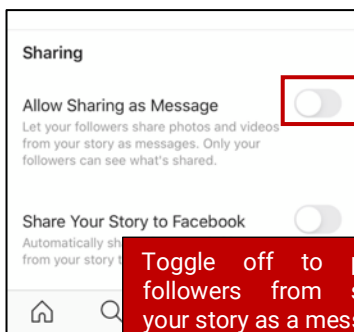
Toggle off to prevent followers from sharing your story as a message.
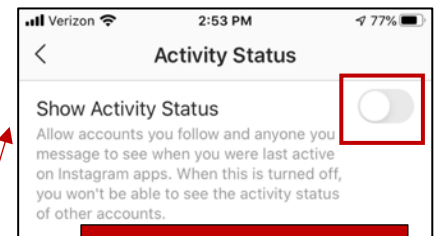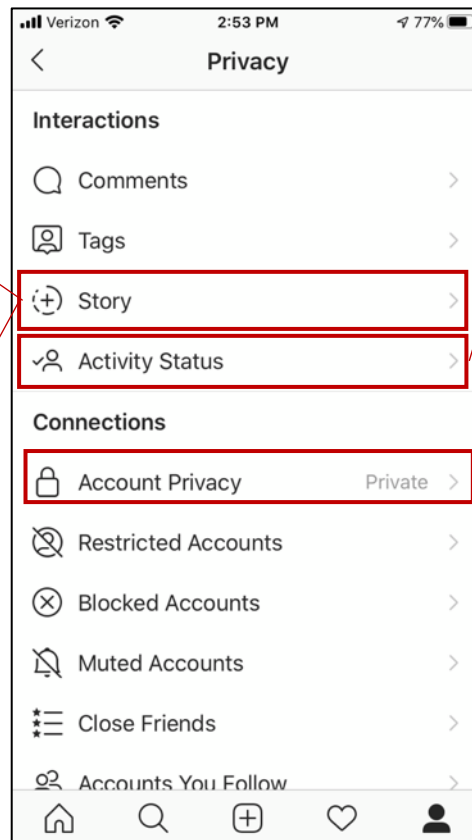
Toggle off so others cannot see when you are active on Instagram apps.

Toggle on to keep your account private so only people you approve can see your photos and videos.

SECURITY SETTINGS
TWO-FACTOR AUTHENTICATION and APPS AND WEBSITES

Settings

- +🧑 Follow and Invite Friends
- 🔔 Notifications
- 🔒 Privacy
- ☑ **Security**
- 💳 Payments
- 📢 Ads
- 👤 Account
- ❓ Help
- ⓘ About

Logins

Security (Verizon 2:54 PM 77%)

Login Security
- 🔑 Password
- 📍 Login Activity
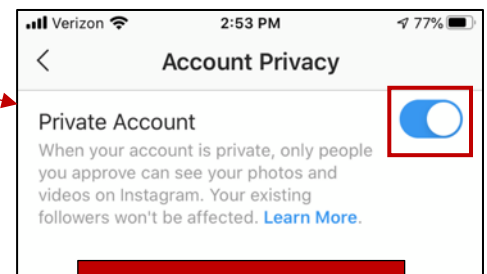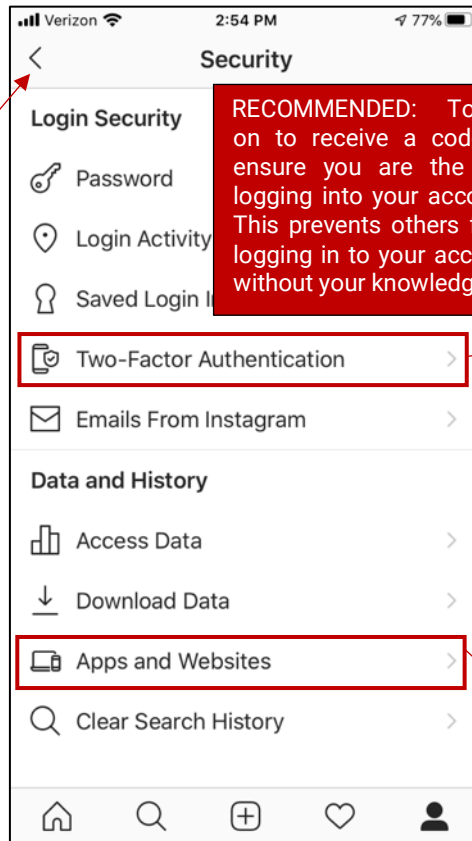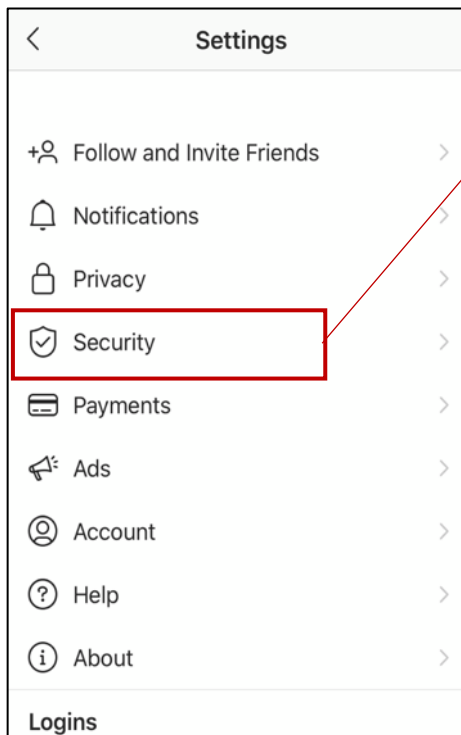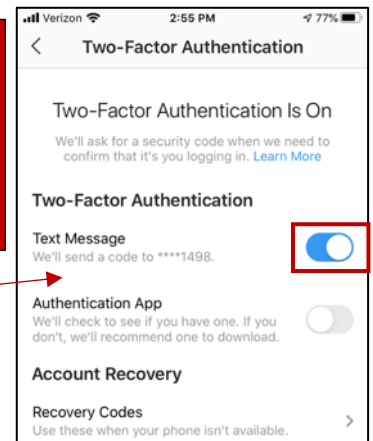- 👤 Saved Login I...
- 📱 Two-Factor Authentication
- ✉ Emails From Instagram

Data and History
- 📊 Access Data
- ↓ Download Data
- 💻 Apps and Websites
- 🔍 Clear Search History

RECOMMENDED: Toggle on to receive a code to ensure you are the one logging into your account. This prevents others from logging in to your account without your knowledge.

Two-Factor Authentication (Verizon 2:55 PM 77%)

Two-Factor Authentication Is On

We'll ask for a security code when we need to confirm that it's you logging in. Learn More

Two-Factor Authentication

Text Message
We'll send a code to ****1498.   [toggle on]

Authentication App
We'll check to see if you have one. If you don't, we'll recommend one to download.   [toggle off]

Account Recovery

Recovery Codes
Use these when your phone isn't available.

Review which apps or websites have access to your Instagram account.

THINGS TO REMEMBER

- **MAKE YOUR ACCOUNT PRIVATE** - Instagram accounts are accessible to the public; therefore, anyone can view your profile, photos, videos, and stories and comment on them. To allow only approved followers to be able to view your posts, set your account to private.
- **HIDE ACTIVITY STATUS** – Individuals you follow or have direct conversations with can by default see when you were last active on Instagram. Turn off the visibility of your status.
- **REMOVE FOLLOWERS** – Remove individuals or followers from your friends list if you no longer want them to see your new posts. This can work for both public and private accounts.
- **HIDE STORIES/RESTRICT DIRECT MESSAGING AND SHARING** – If you don't want to share photos or videos with all followers select specific individuals e.g. family.
- **BLOCK COMMENTS** – If you are annoyed by the constant inappropriate comments on your posts, you can stop this by blocking individuals from commenting.
- **REMOVE TAGS –** Remove or disable your tagging option in settings to prevent posts you are tagged in from automatically being added to your Instagram profile by default.

PASSWORD RECOMMENDATIONS

- Minimum of 8 characters is recommended.
- Use a combination of upper and lowercase letters, numbers and symbols/punctuation marks.
- Enable two-factor authentication when available.
- Should not contain your name, username, phone number, birthday, pets' names or other personal information.
- Should be unique to each app or website you use.
- Don't use common words (dictionary, iloveyou, password) or series of letters (qwerty, abcd1234).
- Using a longer passphrase or series of words may be easier to remember and more secure.

USEFUL LINKS

A Parent's Guide to Internet Safety
www.fbi.gov/stats-services/publications/parent-guide

Wired Kids
www.wiredkids.org

Microsoft Safety & Security
https://support.microsoft.com/en-us/help/4091455/windows-protect-privacy-internet

OnGuard Online
https://www.consumer.ftc.gov/features/feature-0038-onguardonline

Instagram Privacy Settings and Information
https://help.instagram.com/196883487377501