

Instagram Privacy and Safety Checklist

Purpose: A ten-minute checklist to lock down your own Instagram account, vet follow requests, avoid "private account viewer" scams, and help a young person stay safe. Settings names change, so use the search box in Instagram's settings if you cannot find an option.

1. Lock down your account

- ☐ Account is set to private (Settings and privacy, then Account privacy), or I have chosen to stay public on purpose.
- ☐ I have checked what my profile picture, name and bio show to everyone, and removed phone numbers, addresses and school or workplace details.
- ☐ I have reviewed who can tag and mention me.
- ☐ I have reviewed my message settings and who can send me messages.
- ☐ I have checked whether my posts are shared to other apps with different privacy settings.

2. Secure your login

- ☐ My password is unique and not used anywhere else.
- ☐ Two-factor authentication is on, using an authenticator app where possible.
- ☐ I have checked the list of devices logged in to my account and logged out any I do not recognise.
- ☐ My email account linked to Instagram is also protected with two-factor authentication.
- ☐ I know that Instagram will never ask for my password in a direct message.

3. Review your followers

People who followed before you went private can still see your posts unless you remove or block them.

1. Open your followers list.
2. Remove anyone you do not know or no longer trust.
3. Block anyone who has been a problem.
4. Repeat every three months.

4. Vetting a follow request

Tick at least four before approving a stranger.

- ☐ The profile has a real-looking picture and a believable name.
- ☐ It has posts that look genuine, not just reposts or adverts.
- ☐ Followers and following numbers look normal.
- ☐ We have mutual followers I recognise.
- ☐ The account is not new, empty or full of strangers.
- ☐ I know who they are in real life, or have a good reason to accept.

Remember: followers can screenshot what you share.

5. Spotting a "private account viewer" scam

- ☐ It promises to show private photos from just a username (Instagram does not allow this).
- ☐ It shows fake "scanning" screens.
- ☐ It asks for a survey, an app download or a phone number.
- ☐ It asks me to log in with Instagram.
- ☐ It charges a fee or "membership".

If any box is ticked, close the page. Do not enter details.

If you already did:

1. Change your Instagram password and your email password.
2. Turn on two-factor authentication.
3. Log out of unknown devices.
4. Uninstall anything you downloaded and run a security scan.
5. Tell your bank if you paid or shared card details.
6. Warn friends if odd messages were sent from your account.

6. If you want to see a private account

1. Send a follow request.
2. Or ask the person directly, honestly and politely.
3. Or ask a mutual contact to pass on your request.
4. Respect a no. Do not make new accounts or send repeated requests.

7. Helping a young person

- ☐ We have looked through their privacy settings together.
- ☐ Their account is private and they know why.
- ☐ I have read Instagram's current guidance on Teen Accounts and supervision.
- ☐ They know not to share their location, school or phone number.
- ☐ They know they can tell me about anything that worries them without getting into trouble.
- ☐ They know how to block, report and restrict someone.
- ☐ We have agreed what to do if a stranger asks for photos or to move to another app: do not reply, take a screenshot, tell an adult.

If a child may be in immediate danger, call 999.

8. Quarterly check

Date checked	Followers reviewed	Settings reviewed	Notes
--------------	--------------------	-------------------	-------

Want a hand putting this into practice?

Delivered Social is a social media, SEO and web agency based in Guildford and Portsmouth. Say hello at deliveredsocial.com/contact/ and we will point you in the right direction.