Social Media Security

Protect your accounts from hijacking, impersonation and harassment.

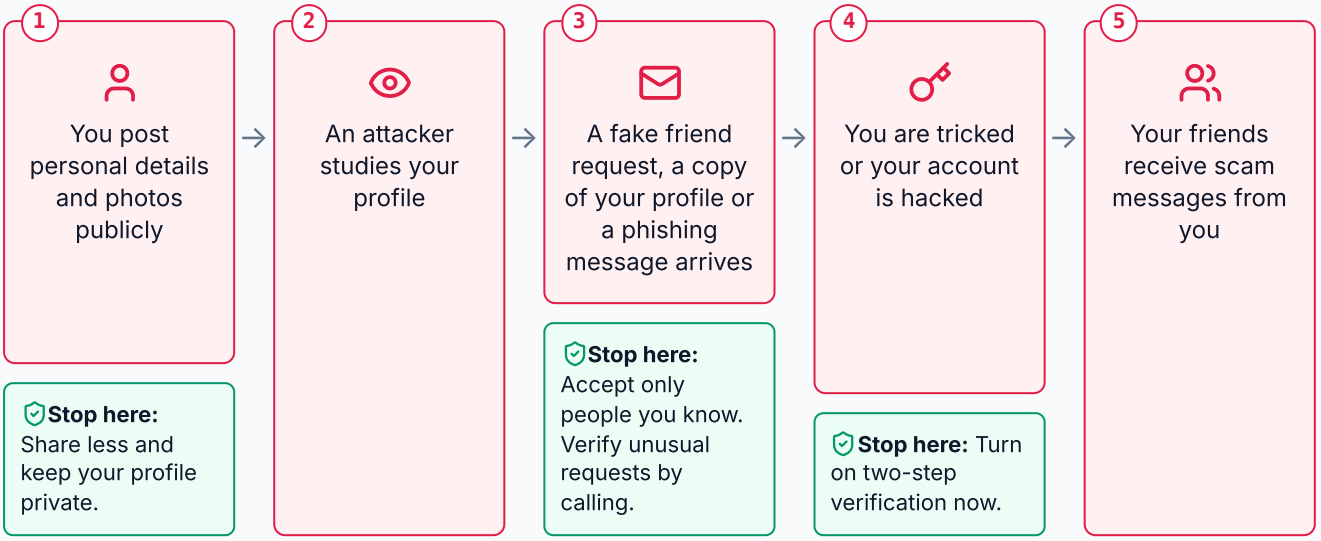
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

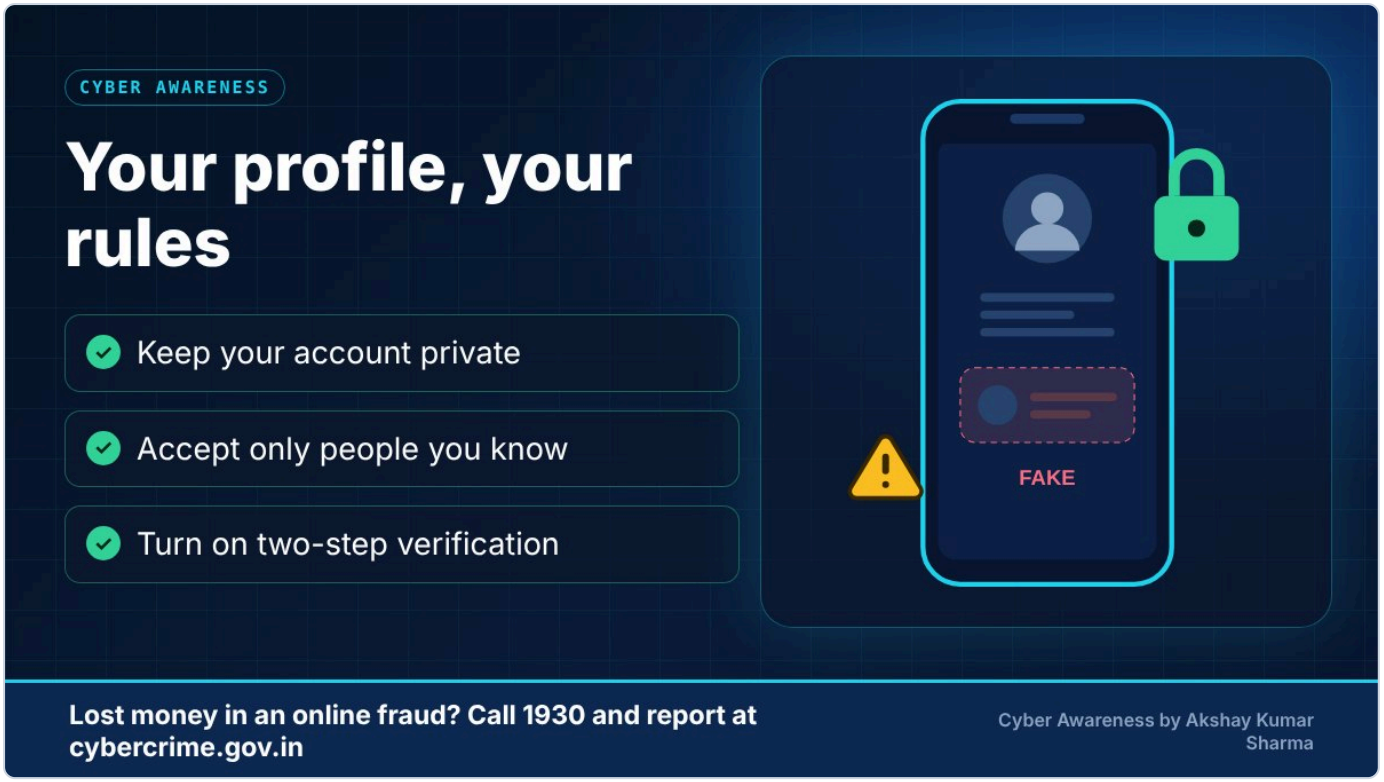
What it is

Social media accounts hold your identity, photos and contacts. Attackers hijack accounts to scam your friends, create fake profiles using your photos, or use what you post to guess passwords and security answers.

How it works - and where you can stop it

Red boxes show what the attacker does. Green boxes show where you can break the chain.





Common warning signs

- ⚠ Login alerts or password-reset emails you did not request.
- ⚠ Friends receive odd messages from your account, such as requests for money.
- ⚠ A friend request or message from someone who copies a person you already know.
- ⚠ Messages with links that promise free followers, prizes or 'see who viewed your profile'.
- ⚠ Unknown devices appearing in your account's login history.

Practical prevention tips

- Use a strong, unique password and turn on two-factor authentication.
- Review privacy settings regularly and limit who can see your personal details.
- Do not accept requests from strangers or log in through links sent in messages.
- Be careful with third-party apps that ask for access to your account.
- Avoid posting information that doubles as a security answer, like birthdays or pet names.

Risky habit vs safe habit

RISKY	SAFE
✕ Public profile with phone number, address and birthday	✓ Private profile with minimal personal details
✕ Accept every friend request	✓ Accept people you know and check mutual friends
✕ Click links in messages, even from friends	✓ Ask your friend on a call if the message is genuine
✕ Use the same password everywhere	✓ Use a unique password and two-step verification

What to do if it happens

1. Try to change your password and log out of all devices from the platform's security settings.
2. Use the platform's official account-recovery and report options.
3. Warn your contacts that your account was compromised.
4. Report impersonation, harassment or fraud on the platform and, where needed, at cybercrime.gov.in.

Official reporting resources

- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- CERT-In (Indian Computer Emergency Response Team) - https://www.cert-in.org.in/

Never share your banking password, OTP, UPI PIN, card CVV or full card number with anyone - not even someone claiming to be from your bank, police or a government office. This website will never ask for them.

This website is an educational resource. It is not an official government reporting portal or an emergency response service. If you are a victim of cyber fraud, report it through the official channels listed on each page.
Akshay Kumar Sharma - https://www.youtube.com/@cybersecwithakshay