Digital Footprint and Privacy

What you leave behind online, who can see it, and how to reduce the risk.

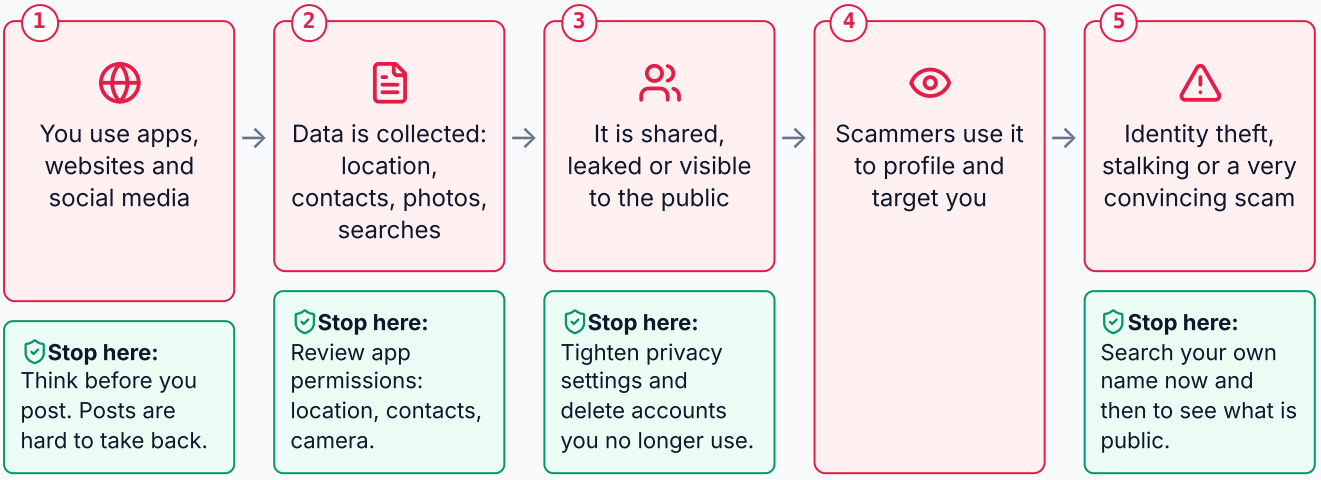
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

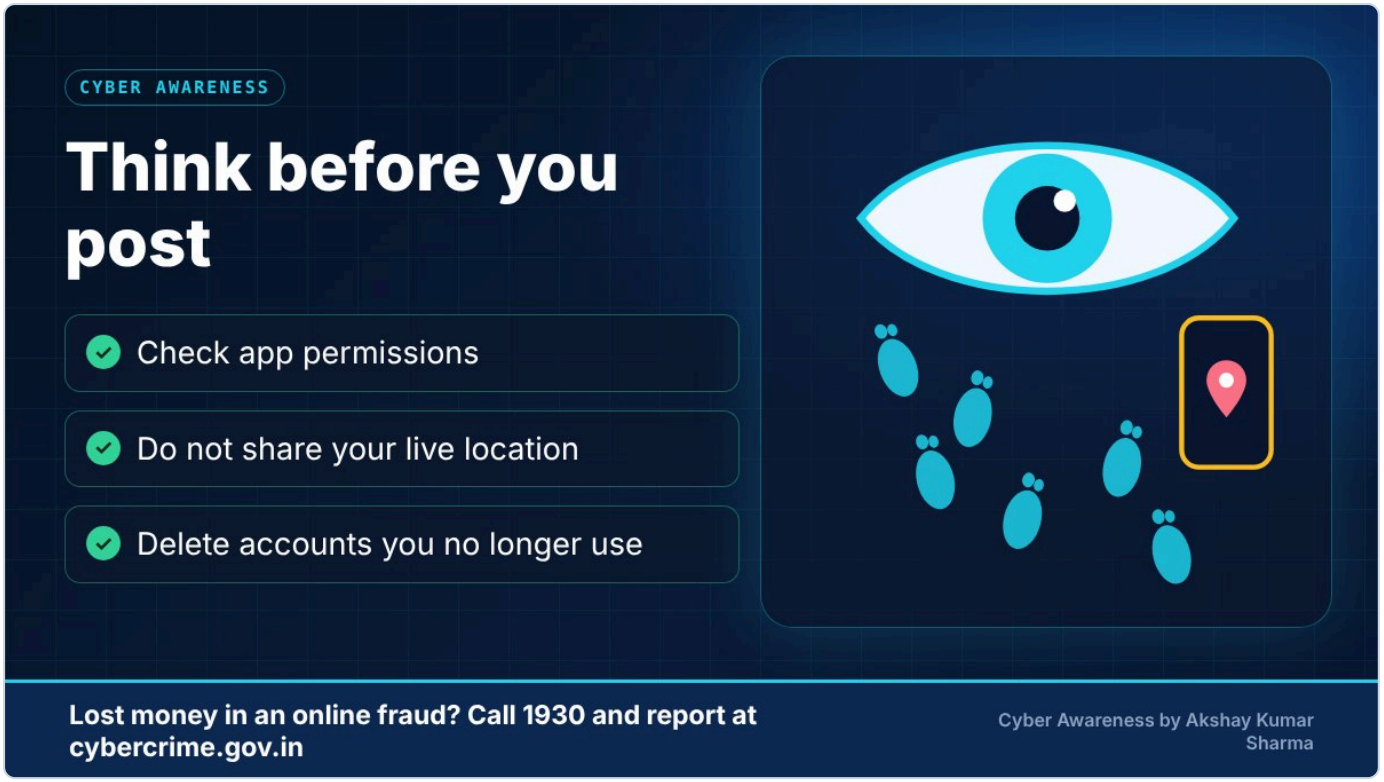
What it is

Your digital footprint is the trail of information about you online: posts, photos, comments, app data, location, and the information websites collect. Scammers and stalkers can combine small pieces to impersonate you or target you.

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

- ⚠ Apps ask for permissions they do not need, such as contacts or location for a simple tool.
- ⚠ Public profiles show your phone number, address, school or workplace, or daily routine.
- ⚠ You often share photos of documents, tickets or cards online.
- ⚠ Old accounts you no longer use are still active.
- ⚠ Strangers know personal details about you before you tell them.

Practical prevention tips

- Review app permissions and remove those that are not needed.
- Set social profiles to the most private setting you are comfortable with.
- Do not post ID documents, boarding passes, tickets or live location.
- Delete accounts and apps you no longer use.
- Think before you post: once something is shared, you cannot fully control where it goes.

Risky habit vs safe habit

RISKY	SAFE
✕ Give every app every permission	✓ Allow only what the app really needs
✕ Post your live location and travel plans	✓ Share later and only with close people
✕ Use public Wi-Fi for banking	✓ Use mobile data or a network you trust
✕ Send photos of ID documents casually	✓ Share only when needed, and only with a trusted party

What to do if it happens

1. Remove or hide the post or information and ask the site or platform to take it down if needed.
2. Tighten privacy settings and change passwords if personal details were used to guess them.
3. If someone is misusing your information or harassing you, keep evidence and report on cybercrime.gov.in.

Official reporting resources

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