# Password and Account Security

Practical habits for strong passwords, two-factor authentication and safe account recovery.

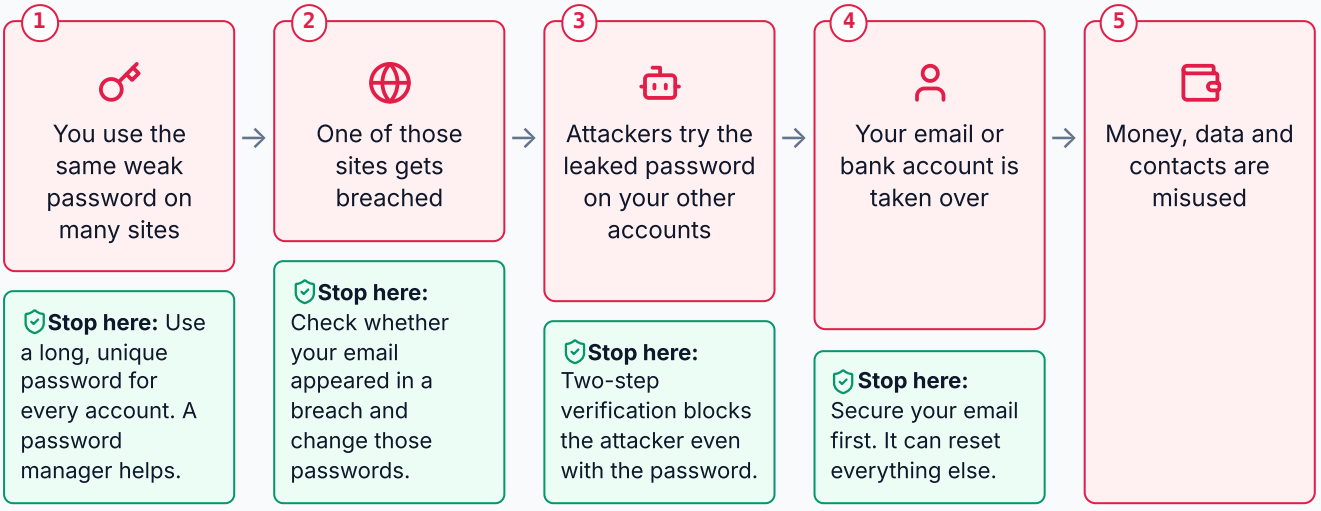
**Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.**

## What it is

A strong password is only one layer. The biggest risks are reusing the same password across sites and falling for phishing. When one website leaks passwords, attackers try the same combination on your email, banking and social accounts.

### 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

- ⚠ You use the same or a similar password on several websites.
- ⚠ Your password is short, a name, a date, or a common word.
- ⚠ You receive security alerts about logins from places or devices you do not recognise.
- ⚠ Your email or phone number appears in a known data breach.
- ⚠ You have never turned on two-factor authentication for email or banking.

## Practical prevention tips

- Use a long passphrase (several unrelated words) or a password manager to create and store unique passwords.
- Never reuse passwords, especially for email, which can reset your other accounts.
- Turn on two-factor authentication, preferably with an authenticator app rather than SMS where possible.
- Keep recovery email and phone number up to date.
- Do not store passwords in plain notes or share them over chat.

### Risky habit vs safe habit

| RISKY | SAFE |
| --- | --- |
| ✕ Use 'password123' or your birth date | ✓ Use a long passphrase of random words |
| ✕ Reuse one password on every site | ✓ Use a different password for each account |
| ✕ Skip two-step verification | ✓ Turn it on, preferably with an authenticator app |
| ✕ Keep passwords in notes or chat apps | ✓ Store them in a trusted password manager |

## What to do if it happens

1. Change the password on the affected account at once and on every site where you reused it.
2. Log out of all sessions and review connected apps and recovery details.
3. Check whether your email appears in a known breach using a trusted checker.
4. If money or identity misuse is involved, report at cybercrime.gov.in (and 1930 for financial fraud).

## Official reporting resources

- CERT-In (Indian Computer Emergency Response Team) - https://www.cert-in.org.in/
- Have I Been Pwned (third-party breach checker) - https://haveibeenpwned.com/

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