Malware and Suspicious Applications

How harmful apps and files get onto devices, and how to keep your phone and computer clean.

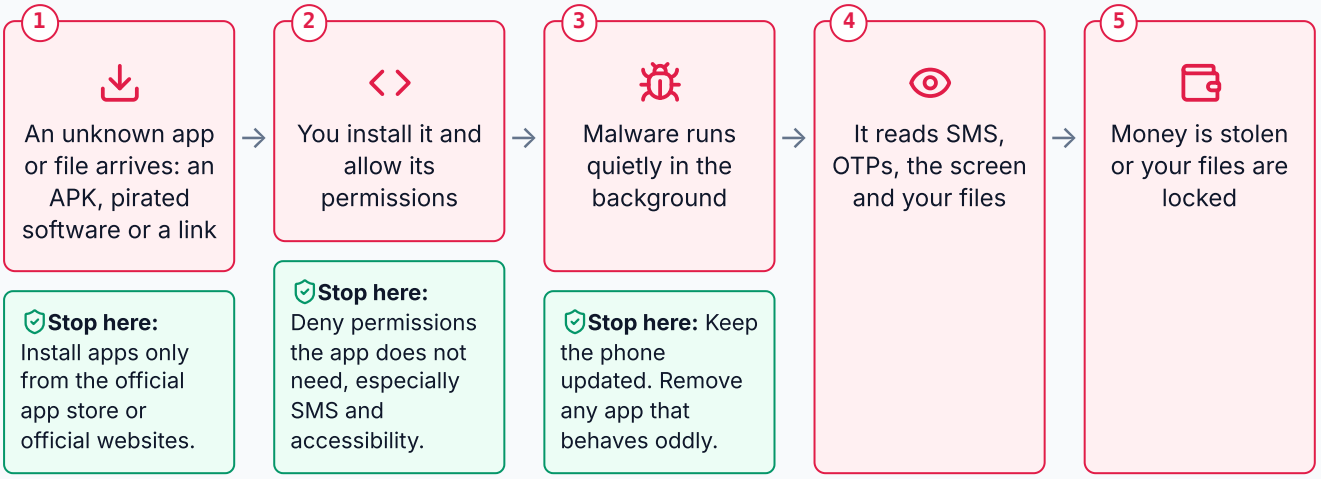
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

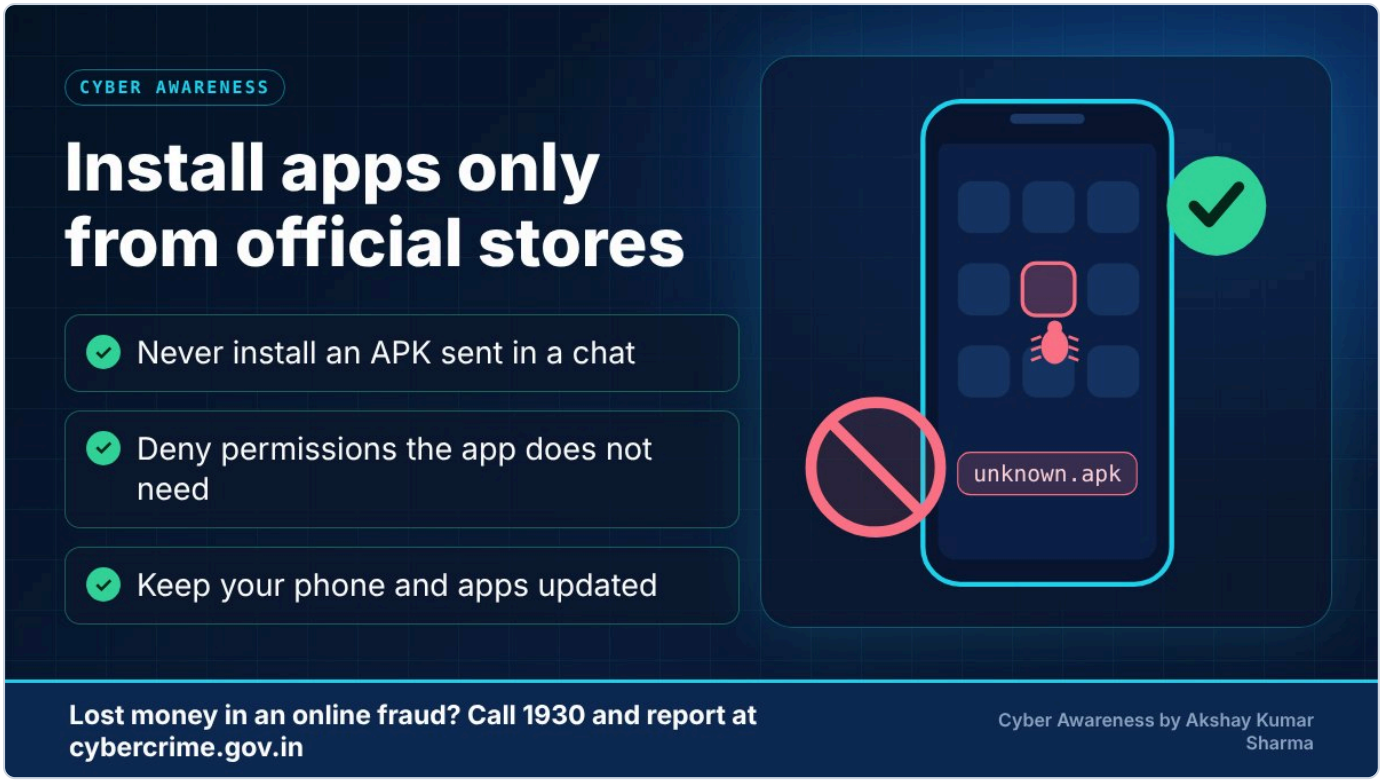
What it is

Malware is software designed to harm or spy on you: stealing passwords, reading messages, locking files or taking over your device. It usually arrives through fake apps, APK files shared in chats, cracked software, or attachments in emails.

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

- ⚠ An app or file sent to you in a chat, asking you to install it outside the official app store.
- ⚠ Apps that ask for accessibility, SMS or device-admin permissions without a clear reason.
- ⚠ Battery draining fast, the device becoming slow, or unknown apps appearing.
- ⚠ Pop-ups, redirects, or messages sent from your number that you did not send.
- ⚠ A 'bank', 'KYC', 'electricity bill' or 'RTO challan' app or APK sent by message.

Practical prevention tips

- Install apps only from the official app store and check the publisher and reviews.
- Never install APK files received through messages, even from contacts.
- Keep your operating system and apps updated, and use a reputable security app.
- Avoid pirated or cracked software.
- Review app permissions and uninstall anything you do not recognise.

Risky habit vs safe habit

RISKY	SAFE
✕ Install an APK sent on WhatsApp or Telegram	✓ Use only the official app stores
✕ Use cracked or pirated software	✓ Use genuine or free open-source software
✕ Ignore system and app updates	✓ Keep your phone and apps updated
✕ Never back up your files	✓ Keep a regular backup, ideally offline as well

What to do if it happens

1. Disconnect from the internet, uninstall the suspicious app and run a security scan.
2. Change passwords from a clean device, starting with email and banking.
3. Contact your bank if the device has banking apps. If needed, back up important data and reset the device.
4. Report to cybercrime.gov.in, and to 1930 if money was lost.

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