Cyber Awareness Guides

Plain-language guides on online threats, with diagrams

By Akshay Kumar Sharma

1. Phishing and Fake Websites
2. UPI and Payment Fraud Awareness
3. OTP and Social Engineering
4. Online Job and Investment Scams
5. Social Media Security
6. Password and Account Security
7. Digital Footprint and Privacy
8. AI-Based Scams
9. Malware and Suspicious Applications
10. Cyber Safety for Students and Families

Educational resource only. Always verify contact details on the official websites listed.

Phishing and Fake Websites

How fake emails, SMS and websites trick you into giving away logins, money or personal details.

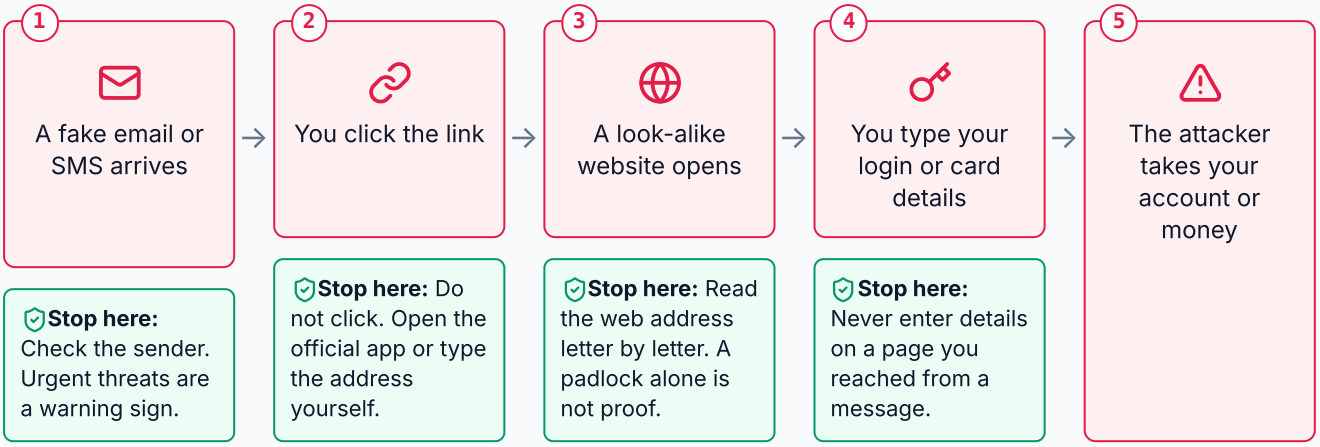
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

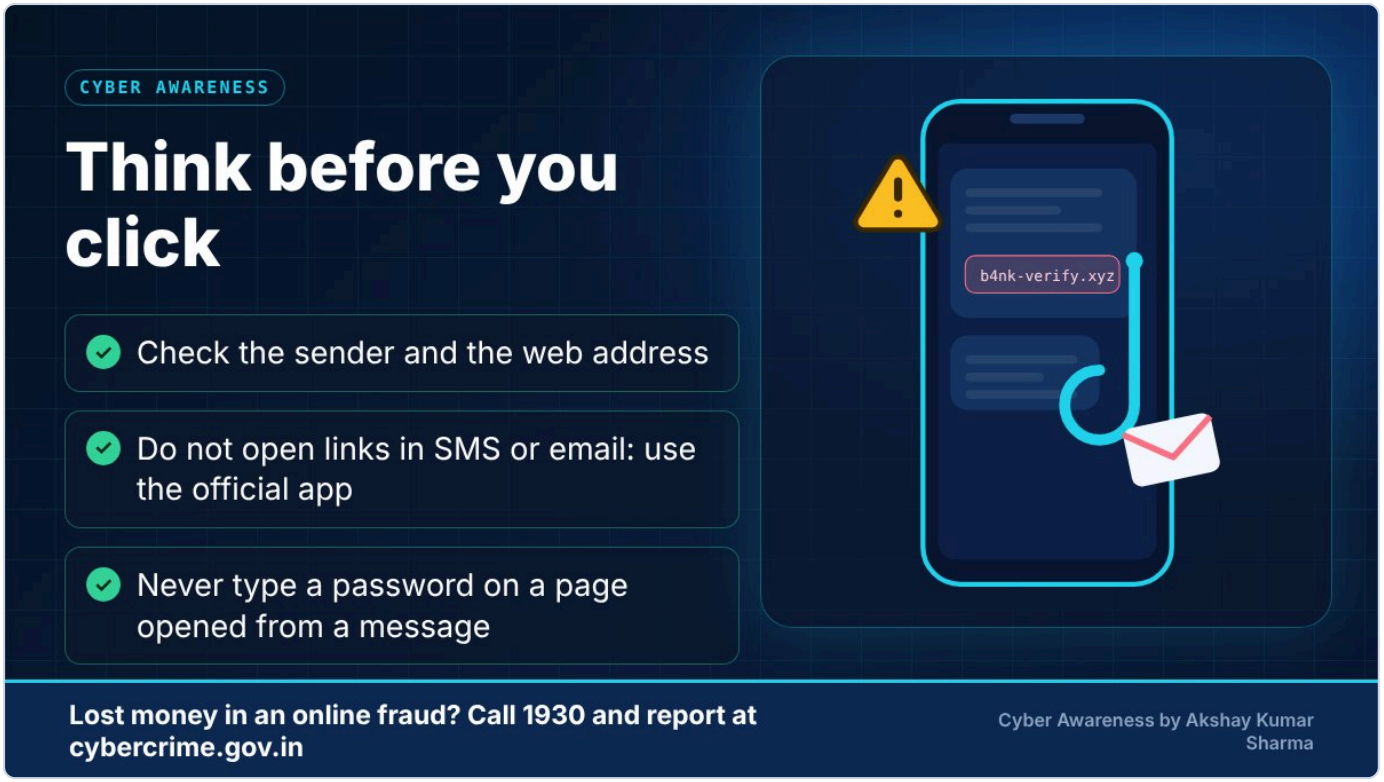
What it is

Phishing is when an attacker pretends to be a trusted organisation - a bank, a courier, a government office or a company you know - to make you click a link, open a file or enter your details. The link often leads to a fake website that looks almost identical to the real one. Anything you type there goes straight to the attacker.

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

- ⚠ Urgent or threatening language: 'Your account will be blocked today', 'Last warning'.
- ⚠ The sender address or website address is slightly different from the real one (extra letters, odd domain endings).
- ⚠ A link or attachment you were not expecting, especially from an unknown number or address.
- ⚠ Requests for passwords, OTP, card details or KYC updates through a link.
- ⚠ Poor spelling, strange formatting, or a login page reached from a message instead of by typing the official address.

Practical prevention tips

- Do not click links in unexpected messages. Open the official app or type the official website address yourself.
- Check the full web address before entering any login. Look for small spelling changes.
- Turn on two-factor authentication on important accounts.
- Keep your phone, browser and security software updated.
- When in doubt, contact the organisation using the number printed on its official website or your card, not the number in the message.

Risky habit vs safe habit

RISKY	SAFE
✕ Click the link in an 'account blocked' SMS	✓ Open your bank's official app directly
✕ Trust a site only because it shows a padlock	✓ Read the full web address carefully
✕ Open attachments you did not expect	✓ Confirm with the sender on a number you already know
✕ Enter your password on a page opened from a message	✓ Type the address yourself or use your bookmark

What to do if it happens

1. If you only clicked the link, close the page, do not enter anything, and run a security scan on your device.
2. If you entered a password, change it immediately on the real website and on any other site where you reused it.
3. If you shared banking or card details, contact your bank at once and then follow the fraud steps below.
4. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
5. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
6. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
7. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
8. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- Sanchar Saathi - report suspected fraud calls/messages (Chakshu) - https://sancharsaathi.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

UPI and Payment Fraud Awareness

Common UPI tricks - fake collect requests, QR code scams and fake refunds - and how to stay safe.

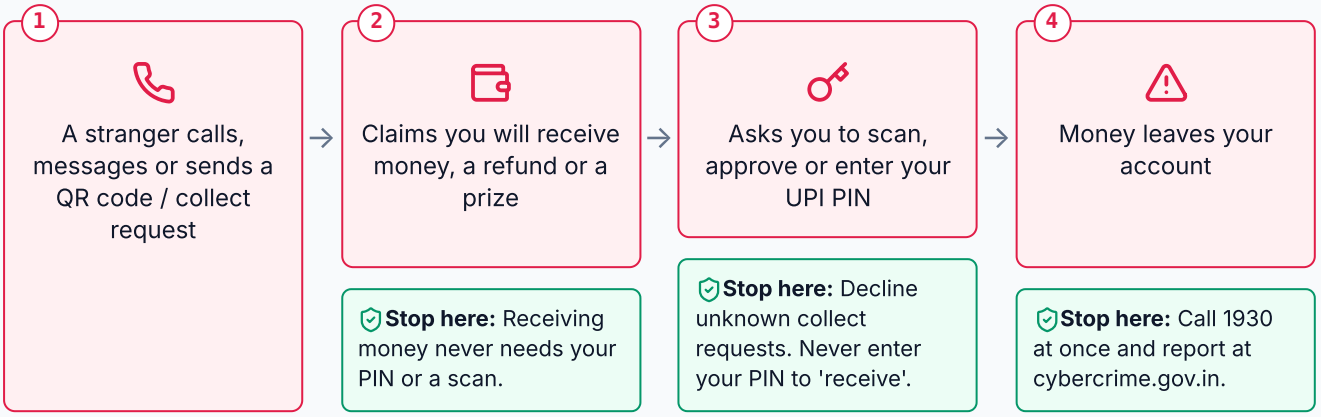
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

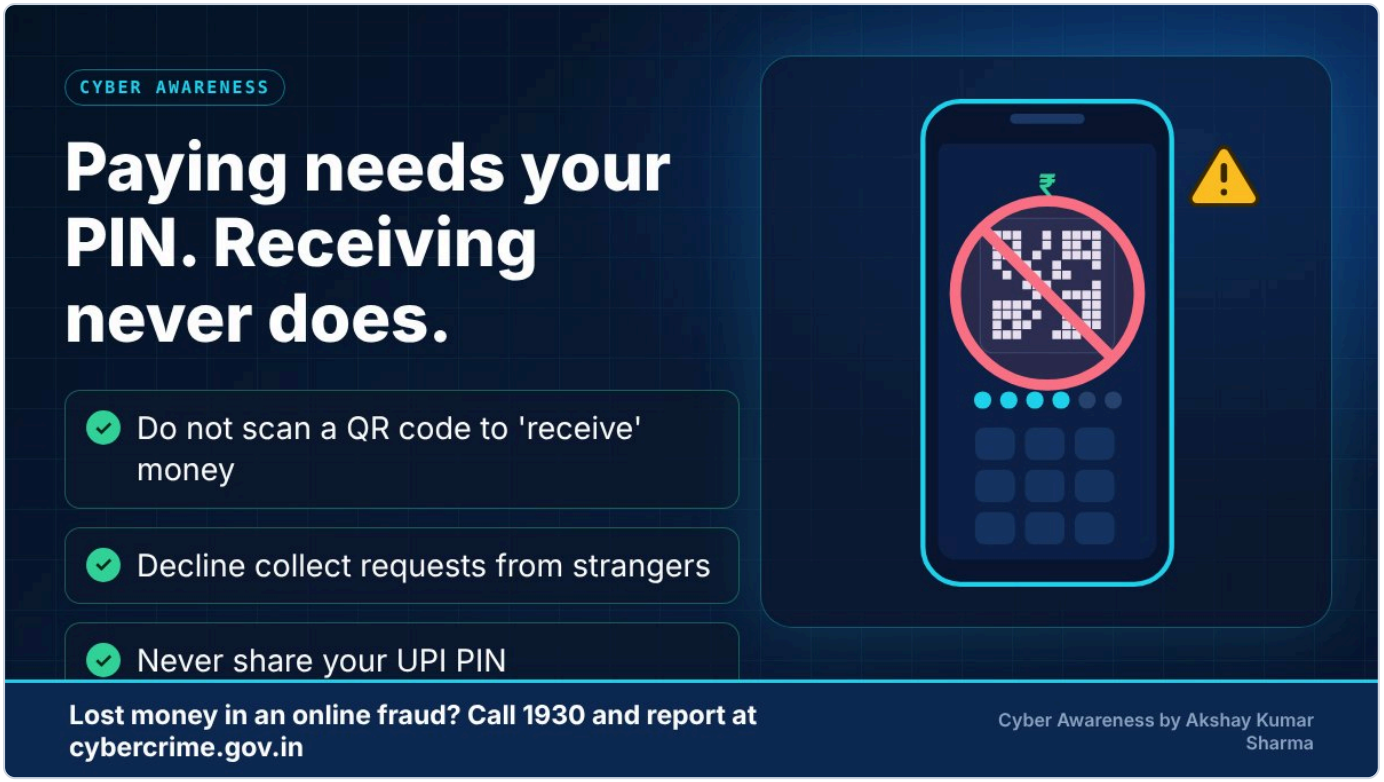
What it is

UPI makes payments fast, which is also why fraudsters like it. A key rule: you enter your UPI PIN only to send money. You never need your PIN to receive money. Scammers rely on confusing people about this, using fake payment requests, QR codes, fake customer-care numbers and 'refund' stories.

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

- ⚠ Someone asks you to scan a QR code or enter your PIN 'to receive' money or a refund.
- ⚠ A 'collect request' appears from an unknown person, or a buyer insists on sending a request instead of paying normally.
- ⚠ A caller claims to be from your bank, a delivery service or a wallet and asks you to install a screen-sharing app.
- ⚠ Customer-care numbers found through search results or social media rather than the official app or website.
- ⚠ Pressure to act immediately, or an offer that is too good to be true.

Practical prevention tips

- Never enter your UPI PIN to receive money. If a screen asks for your PIN, you are sending money.
- Read every payment request carefully and decline requests you did not expect.
- Never install remote-access or screen-sharing apps at someone else's request.
- Get customer-care numbers only from the official app, website or your card.
- Set sensible transaction limits and enable app lock and payment alerts.

Risky habit vs safe habit

RISKY	SAFE
✕ Scan a QR code to 'receive' money	✓ Remember: PIN and scanning are only for paying
✕ Approve a collect request you did not expect	✓ Decline it and report the UPI ID
✕ Call a 'customer care' number found through a search	✓ Use the help section inside the official app
✕ Install a screen-sharing app when 'support' asks	✓ Refuse. Real support does not need remote access to your phone

What to do if it happens

1. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
2. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
3. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
4. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
5. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- NPCI (UPI) - official information - https://www.npci.org.in/
- Reserve Bank of India - public awareness - https://www.rbi.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

OTP and Social Engineering

How attackers manipulate people, not computers - and why an OTP is never meant to be shared.

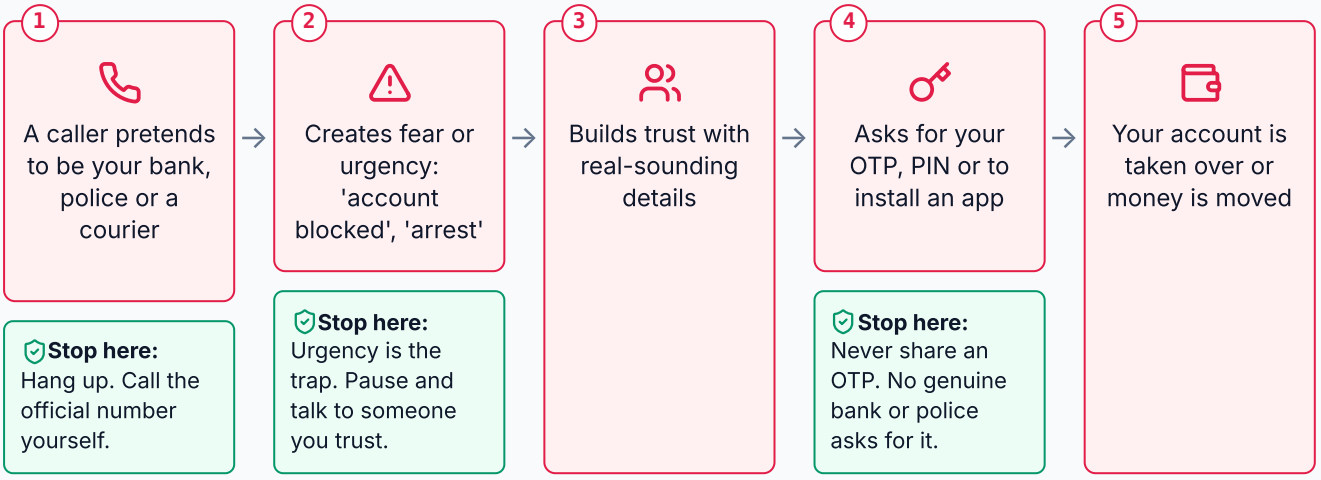
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

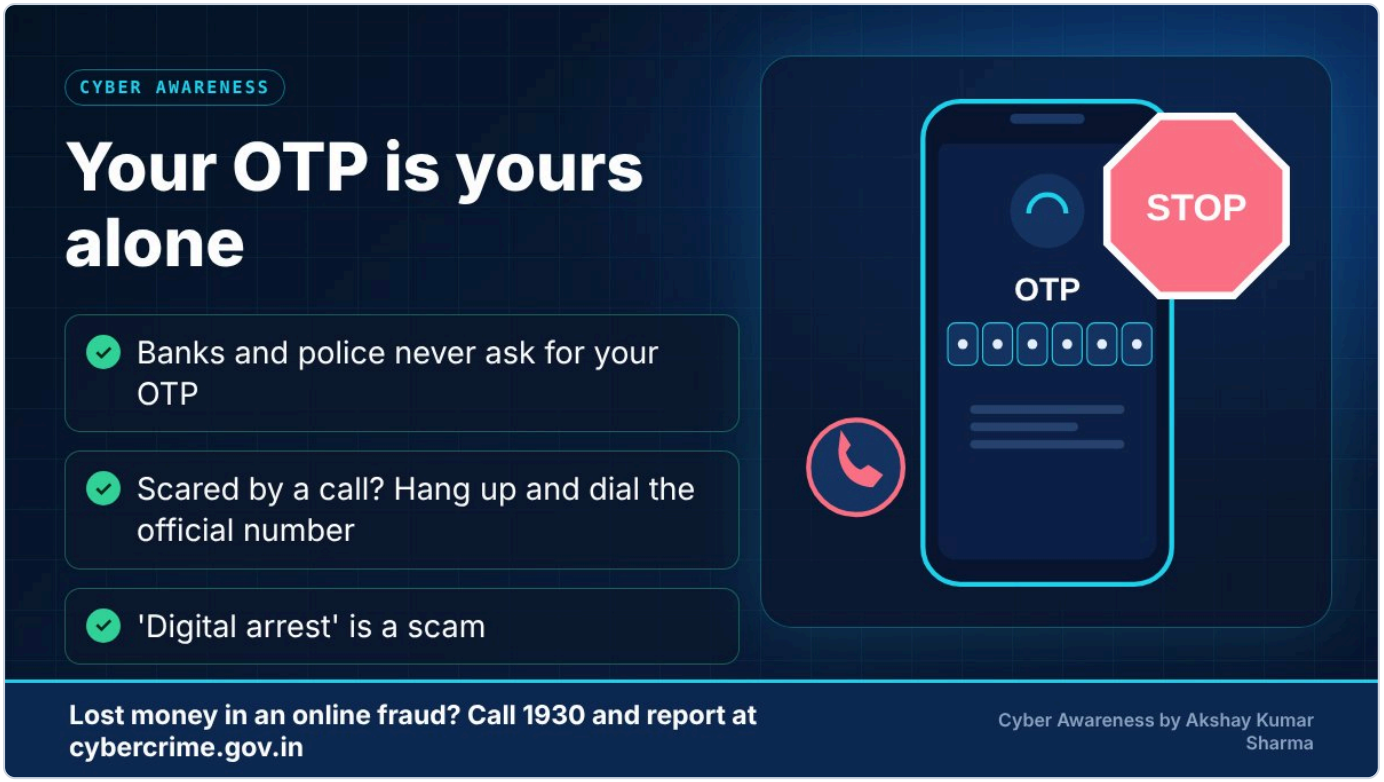
What it is

Social engineering means manipulating a person into giving up information or taking an action, using trust, fear, urgency or greed. An OTP (one-time password) exists to prove that you are the one approving something. If you read it out to a caller, you are approving what the attacker is doing. This includes 'digital arrest' calls, where scammers pose as police or investigation agencies on a call or video call. Authorities have clearly advised that genuine agencies do not arrest people over a video call or demand money to 'settle' a case.

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

- ⚠ A caller claims to be from a bank, police, customs, courier or a government agency and asks for an OTP, PIN or money.
- ⚠ You are told not to disconnect, not to tell family, or to stay on a video call.
- ⚠ Threats such as arrest, account freezing or legal action unless you pay or 'verify' immediately.
- ⚠ A parcel or SIM 'linked to a crime' story that you cannot check independently.
- ⚠ Requests to move money to a 'safe account'.

Practical prevention tips

- Never share an OTP with anyone. A genuine organisation will not ask for it.
- Hang up. Then call the organisation yourself using its official number.
- Do not be rushed. Talk to a family member or friend before acting on any threat.
- Remember: no genuine agency arrests people over video calls or asks for money to close a case.
- Limit what you share publicly - scammers use personal details to sound convincing.

Risky habit vs safe habit

RISKY	SAFE
✕ Share the OTP to 'verify' your account	✓ Keep the OTP private. Only you type it, in the official app
✕ Stay on the line because you are scared	✓ Hang up and call the official number yourself
✕ Believe a 'digital arrest' video call	✓ Know that this is a scam. Call 1930 and report it
✕ Install an app sent on WhatsApp or SMS	✓ Install apps only from the official app store

What to do if it happens

1. Disconnect the call and stop all payments immediately.
2. Report suspected fraudulent calls or messages on Sanchar Saathi (Chakshu).
3. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
4. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
5. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
6. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
7. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Sanchar Saathi - report suspected fraud calls/messages (Chakshu) - https://sancharsaathi.gov.in/
- Reserve Bank of India - public awareness - https://www.rbi.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.

Online Job and Investment Scams

Fake work-from-home jobs, task scams and 'guaranteed return' schemes - how to spot them early.

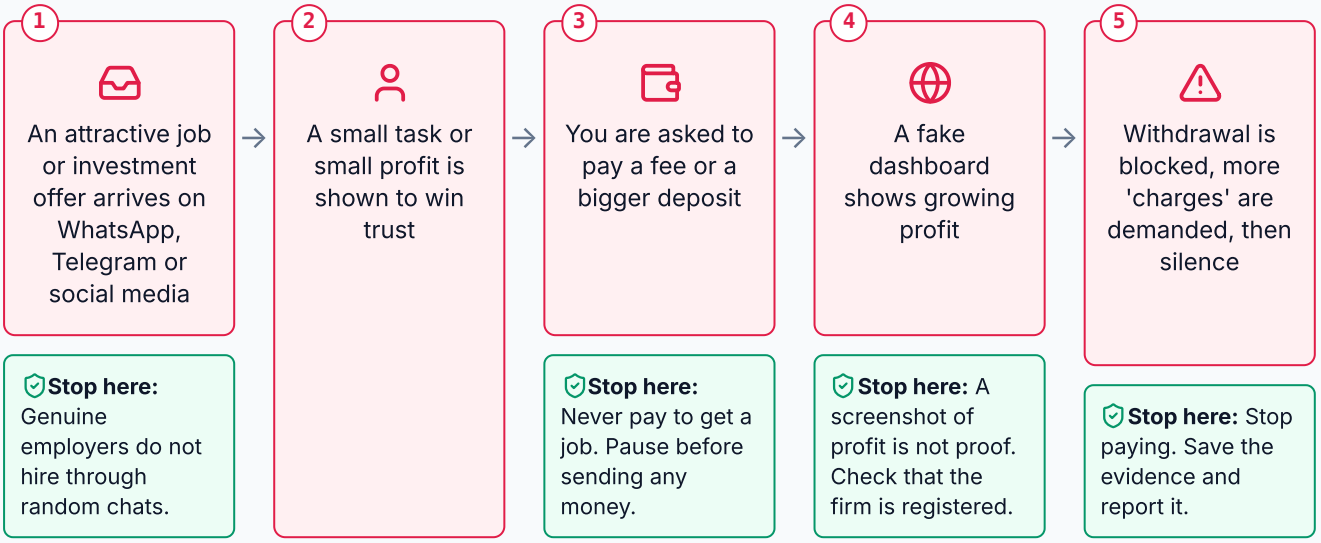
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

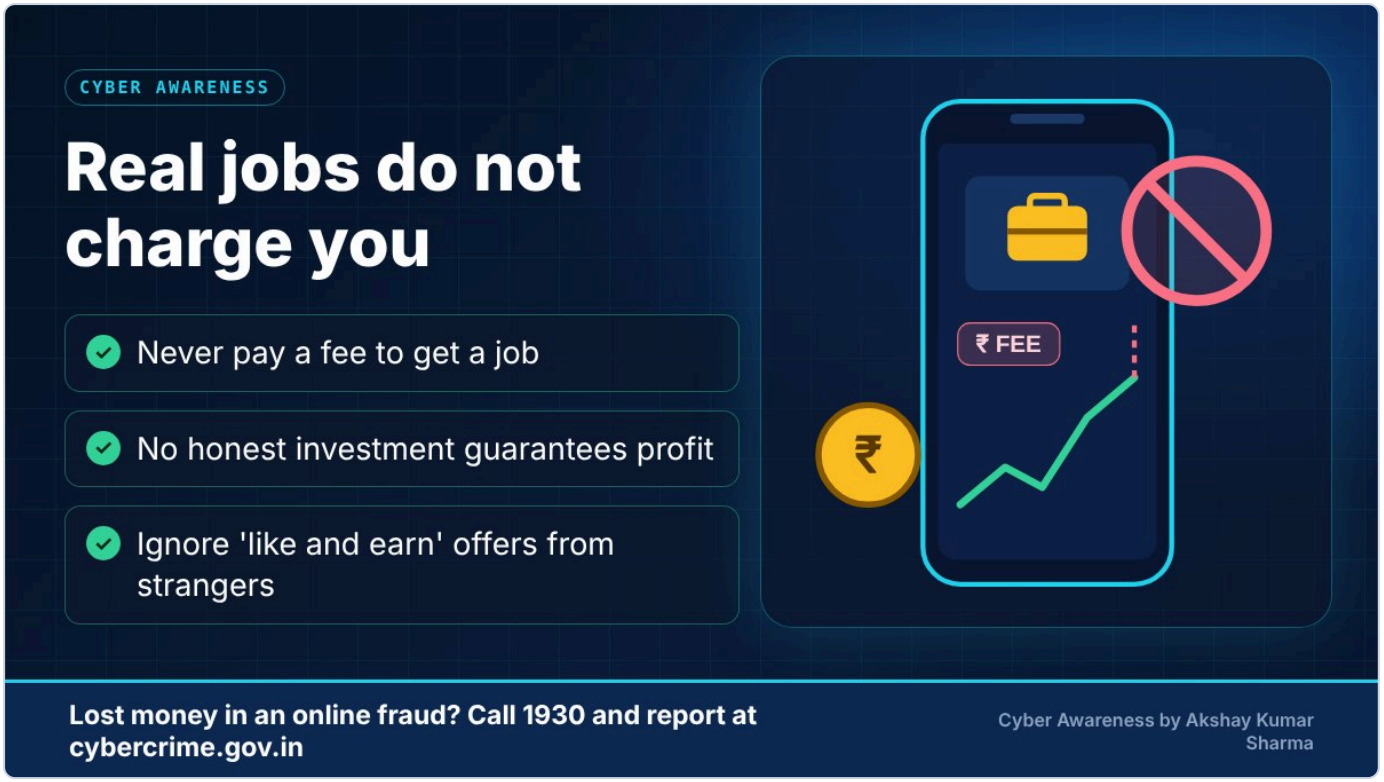
What it is

These scams promise easy money: a part-time job for a few minutes a day, rewards for liking videos, or investments with assured high returns. They often begin on messaging apps or social media. Victims are first shown small 'profits' to build trust, then pushed to deposit larger and larger amounts that they cannot withdraw.

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

- ⚠ Job offers from unknown numbers on WhatsApp or Telegram, with high pay for very simple tasks.
- ⚠ You are asked to pay a 'registration', 'security' or 'processing' fee before you can work or withdraw.
- ⚠ Guaranteed or unusually high returns with little or no risk.
- ⚠ Pressure to deposit more to 'unlock' earlier profits.
- ⚠ No verifiable company details, or an unregulated platform or app link sent in a chat.

Practical prevention tips

- A genuine employer does not charge you to give you a job. Verify the company on its official website.
- Treat 'guaranteed returns' as a red flag. Check that an investment firm or advisor is registered with the relevant regulator.
- Do not join investment groups or install apps shared by strangers.
- Never make payments to personal accounts for jobs or investments.
- Discuss any big financial decision with someone you trust before paying.

Risky habit vs safe habit

RISKY	SAFE
✕ Pay a 'registration fee' for a job	✓ Remember: real jobs do not charge candidates
✕ Trust 'guaranteed' high returns	✓ Know that no honest investment guarantees profit
✕ Join 'tips' groups run by unknown numbers	✓ Use only registered, regulated intermediaries
✕ Do 'like and earn' tasks offered by strangers	✓ Ignore part-time task offers from unknown people

What to do if it happens

1. Stop sending money, even if you are promised that the next payment will release your funds.
2. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
3. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
4. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
5. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
6. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Reserve Bank of India - public awareness - https://www.rbi.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

Social Media Security

Protect your accounts from hijacking, impersonation and harassment.

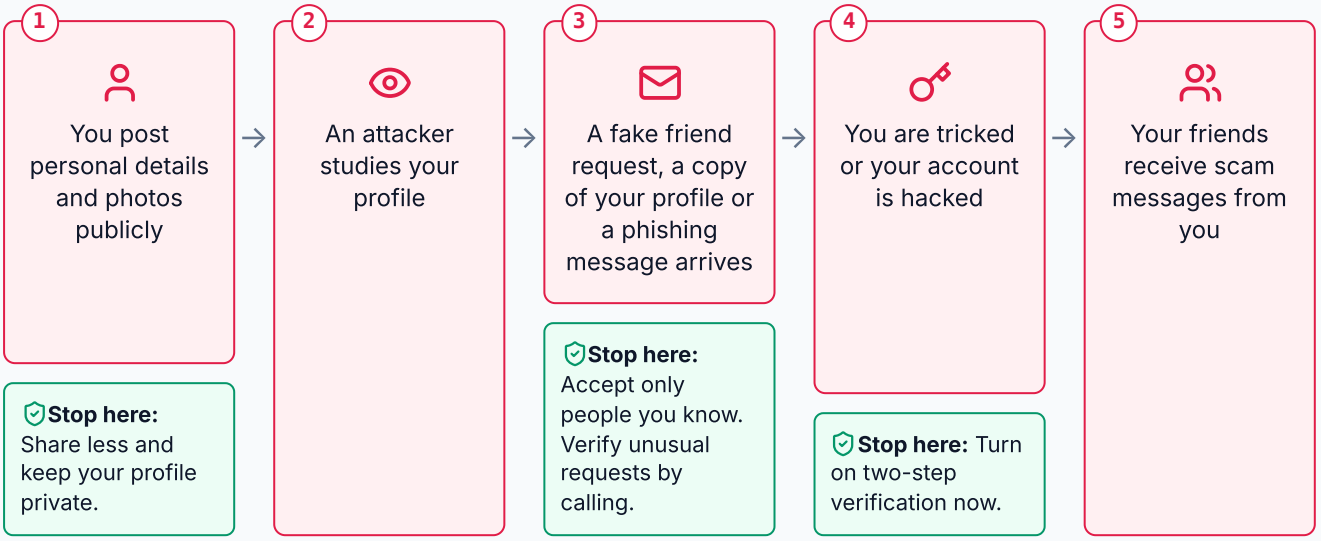
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

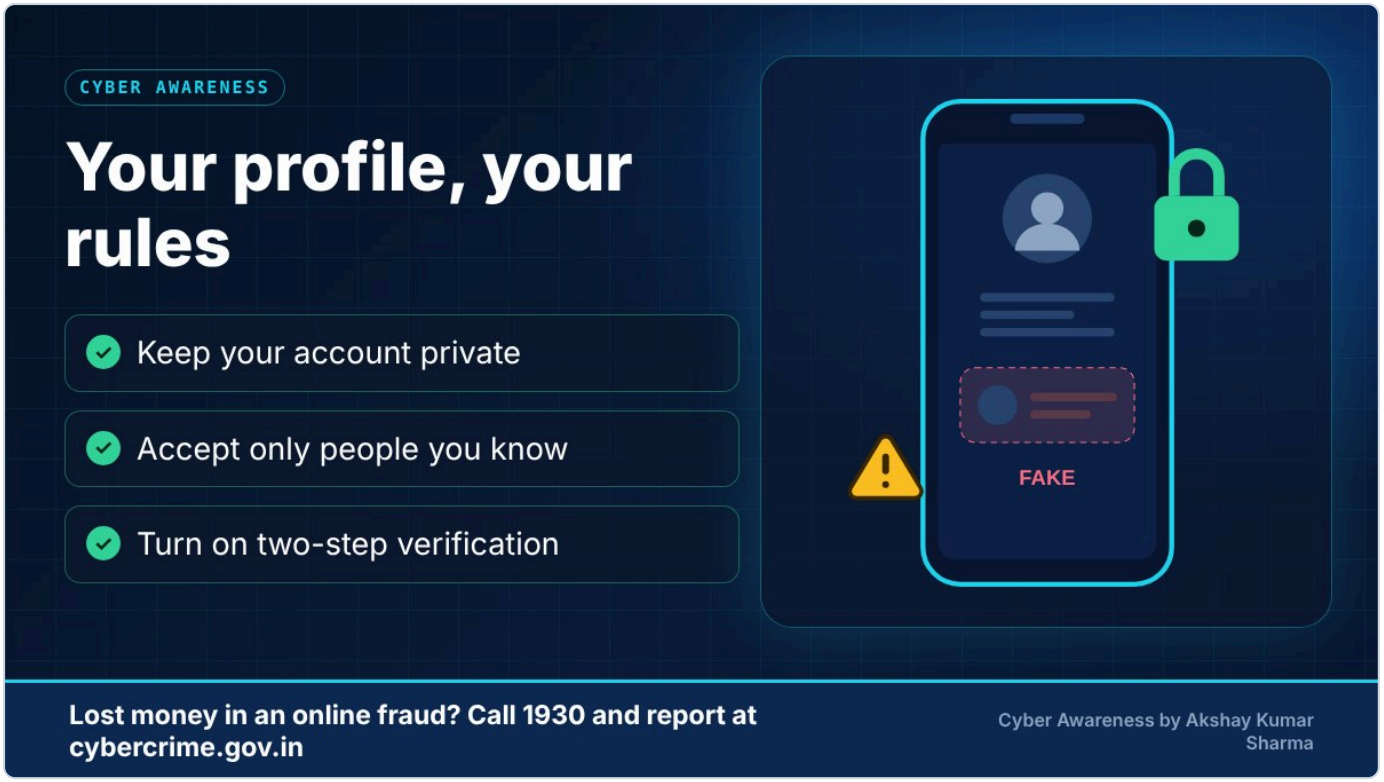
What it is

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

Password and Account Security

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

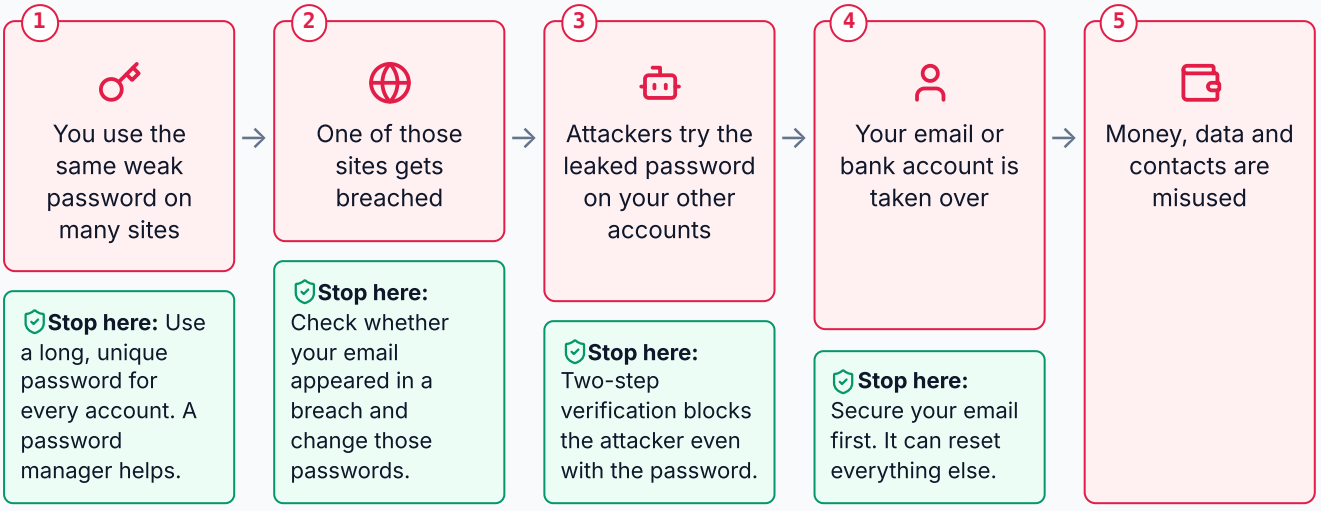
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

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

Digital Footprint and Privacy

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

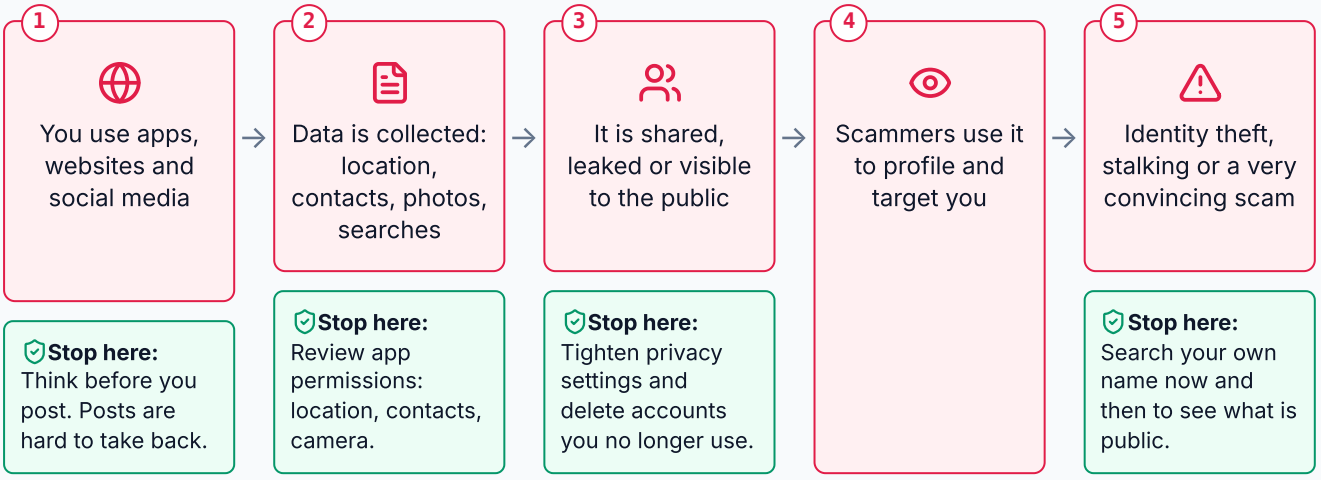
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

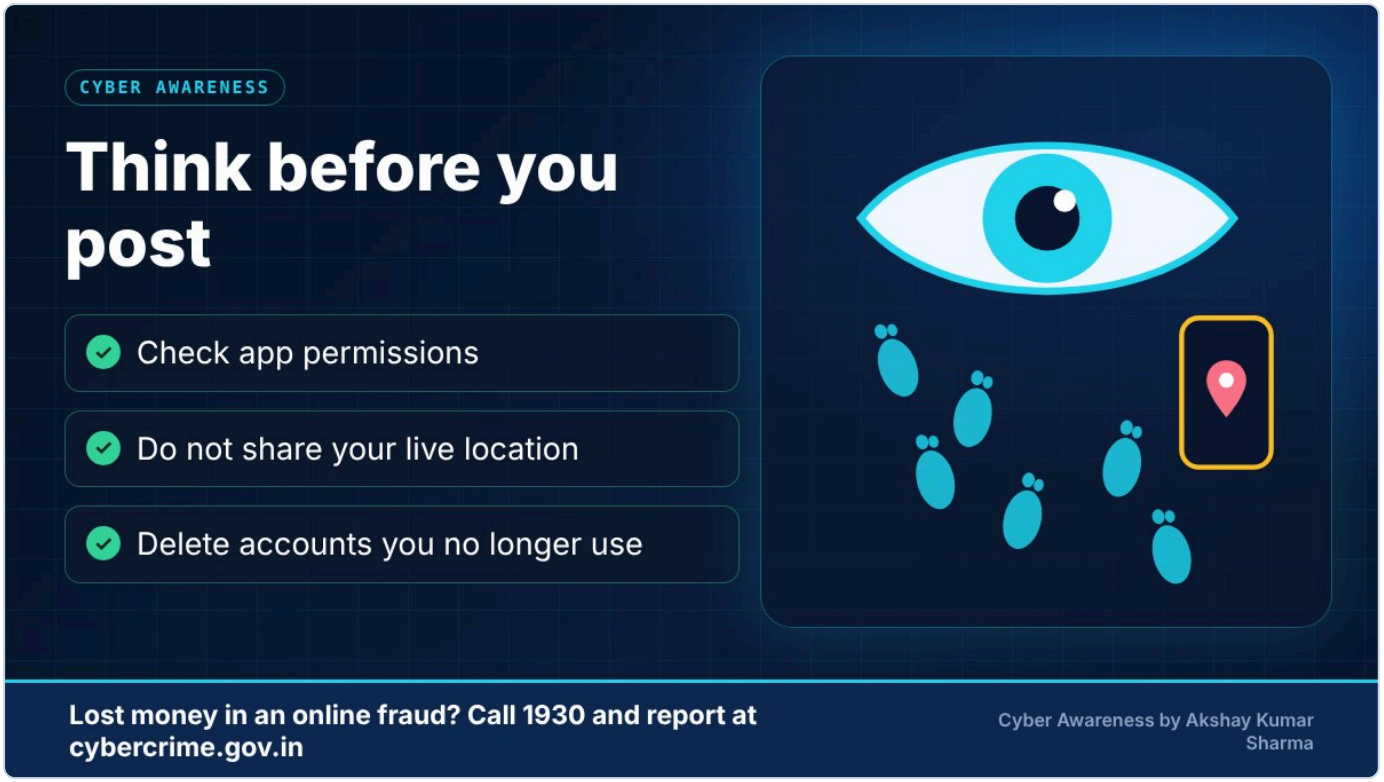
What it is

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

AI-Based Scams

Voice cloning, deepfake videos and AI-written messages - and simple checks that still work.

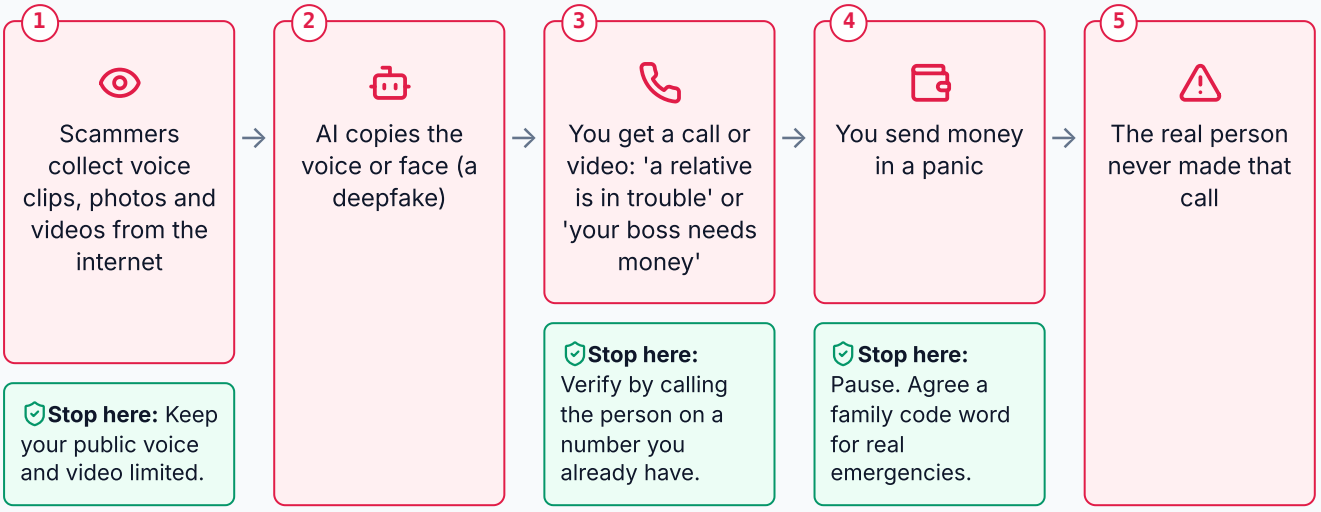
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

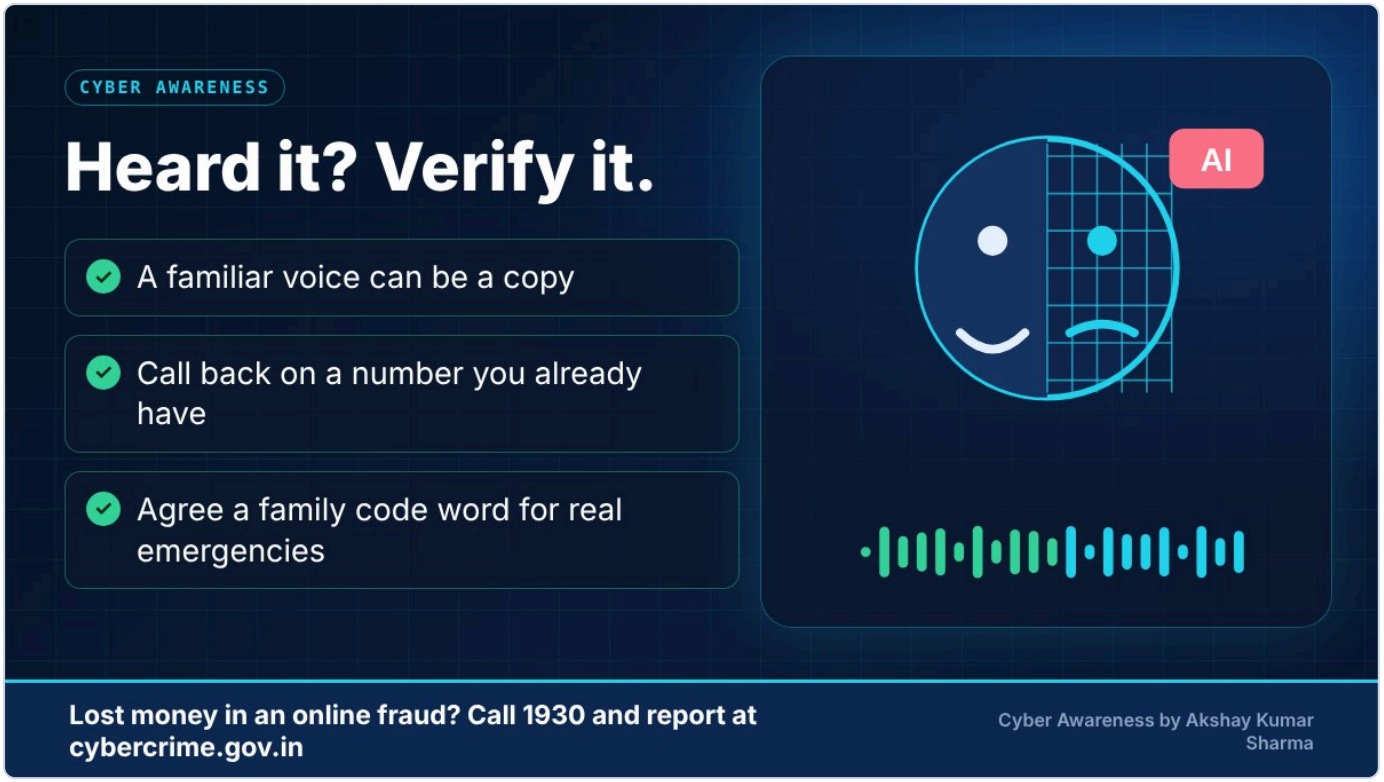
What it is

AI tools make it easier to copy someone's voice, create realistic fake videos, and write convincing messages in any language. A scammer may call in what sounds like a relative asking for urgent money, or share a fake video of a public figure promoting an investment. The technology is new, but the trick is old: trust plus urgency.

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 urgent call or voice note from a 'relative' or 'friend' asking for money, from a new number.
- ⚠ A video or audio of a famous person endorsing a scheme or giveaway.
- ⚠ Messages that are perfectly written but ask for unusual actions or payments.
- ⚠ Video calls where the person's face or lip movement looks slightly off, or the call quality is conveniently poor.
- ⚠ Pressure not to verify through other means.

Practical prevention tips

- Agree on a family 'safe word' or ask a question only the real person could answer.
- Hang up and call the person back on their known number before sending money.
- Be careful with investment promotions featuring celebrities. Verify through official channels.
- Limit public voice and video samples, and keep social profiles private.
- Treat urgency as a warning sign, regardless of how real the voice or face seems.

Risky habit vs safe habit

RISKY	SAFE
✕ Trust a familiar voice on its own	✓ Verify through a second channel
✕ Send money at once for an 'emergency'	✓ Pause and call the person directly
✕ Believe a celebrity video that promotes an investment	✓ Check the official channels of that person or company
✕ Upload your photos to unknown AI apps	✓ Use trusted apps and read their privacy terms

What to do if it happens

1. Stop all payments and verify using another channel.
2. Report the call, message or fake profile on the platform and to Sanchar Saathi if it came by phone.
3. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
4. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
5. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
6. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
7. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- Sanchar Saathi - report suspected fraud calls/messages (Chakshu) - https://sancharsaathi.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.

Malware and Suspicious Applications

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

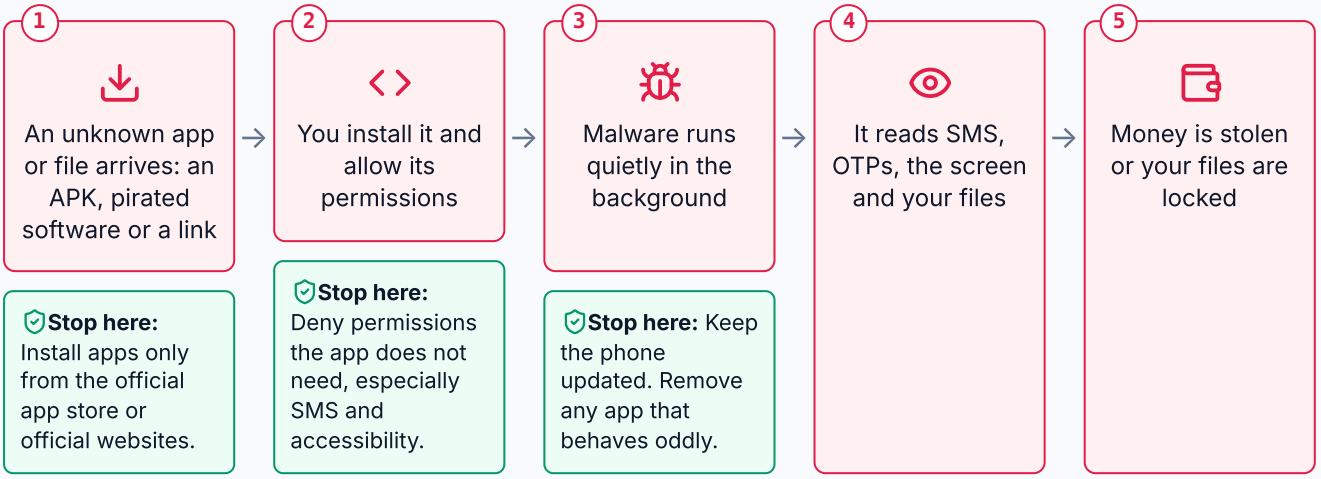
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

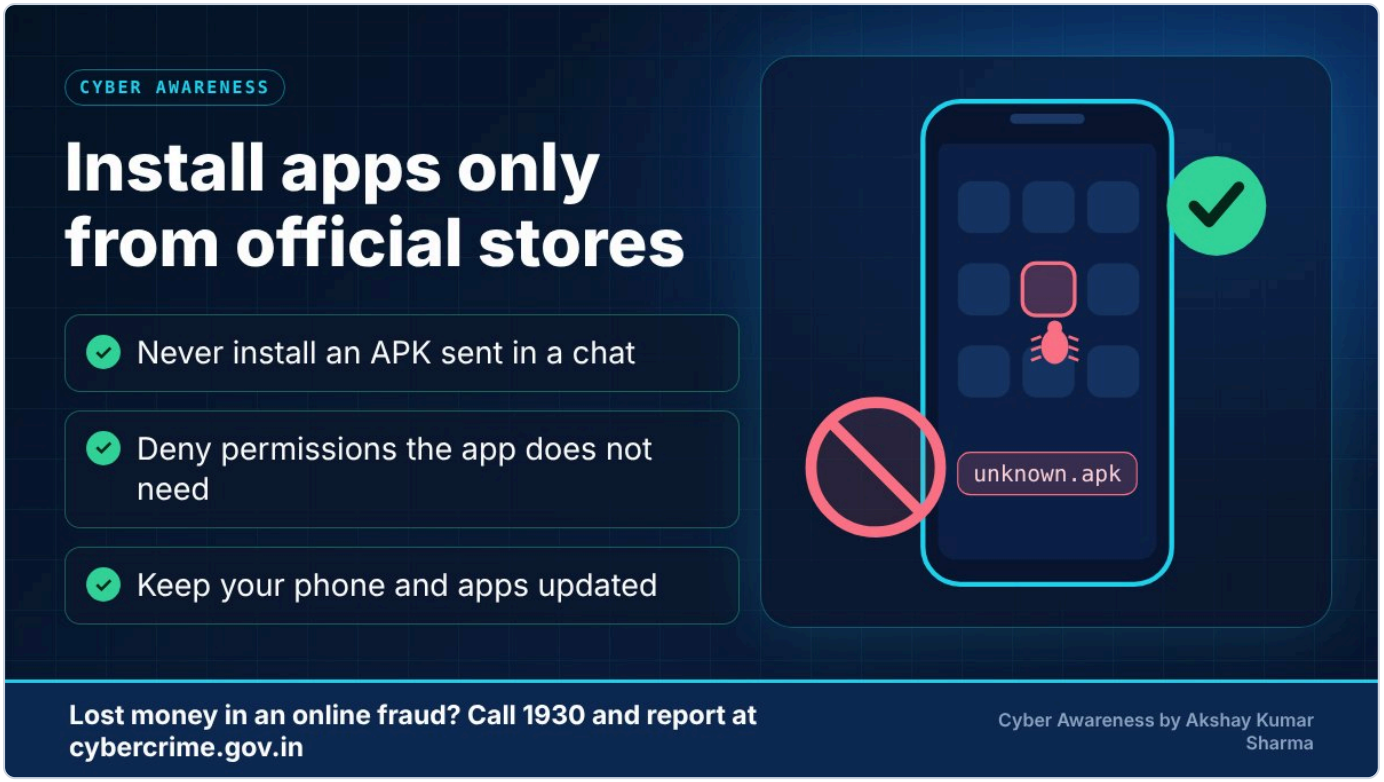
What it is

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

Cyber Safety for Students and Families

Everyday digital safety for students, parents and elders - including online bullying and gaming risks.

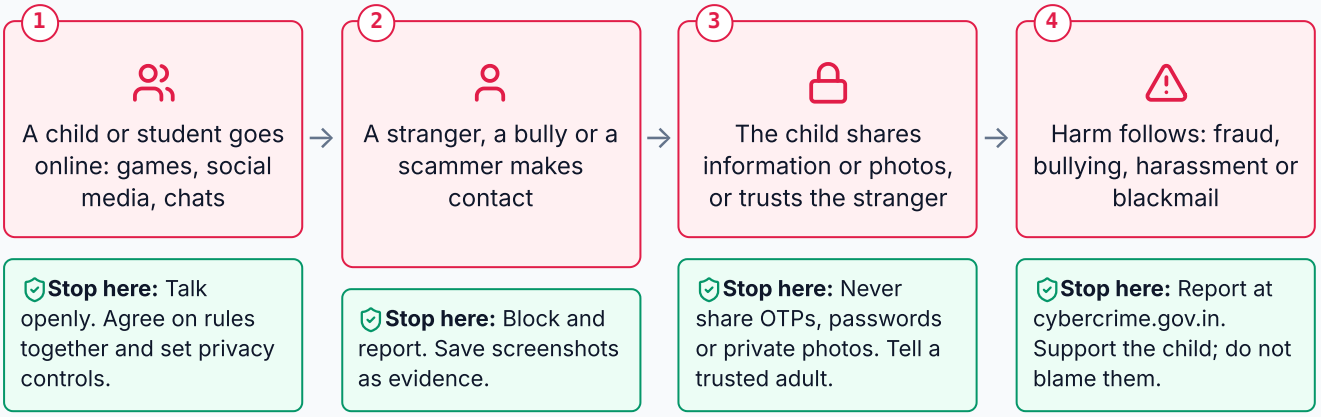
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

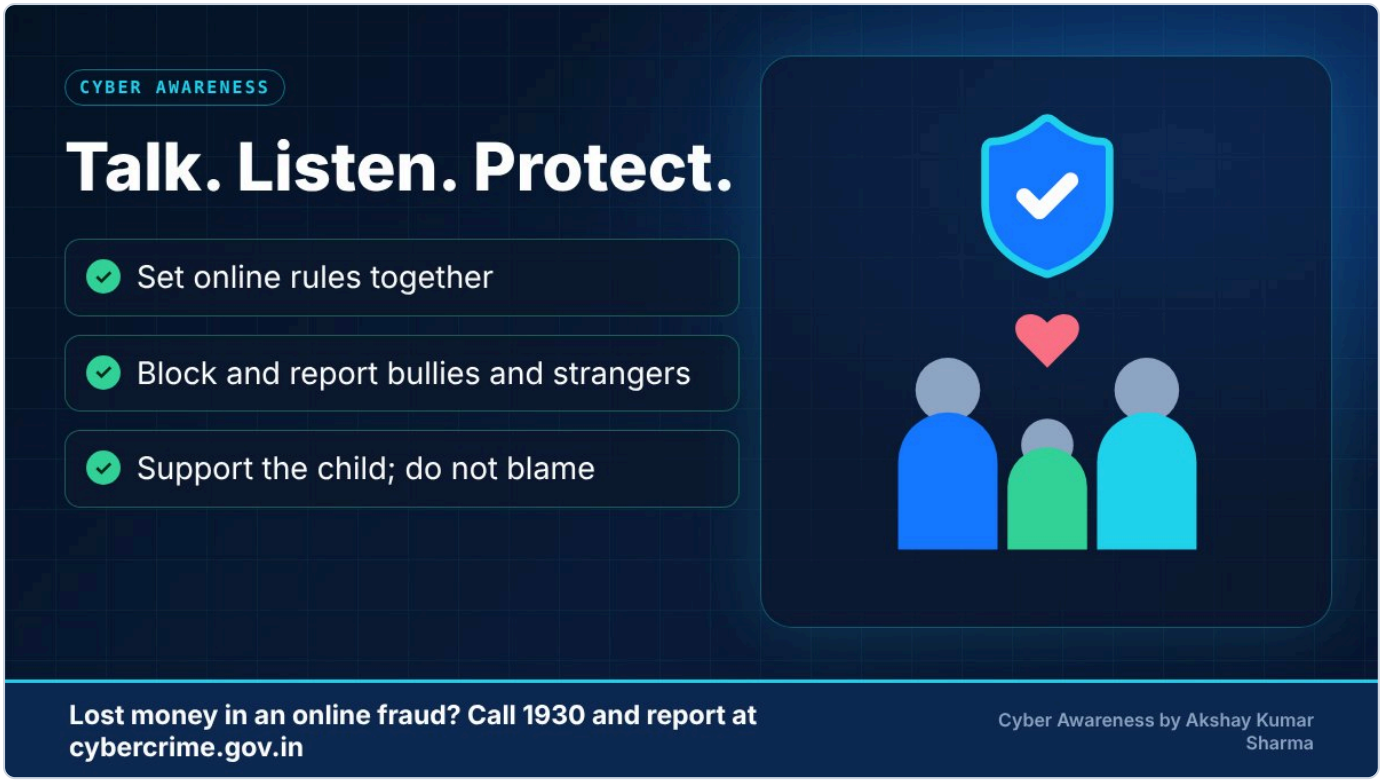
What it is

Students and families are online for learning, gaming, payments and social life. Risks include online bullying, scams promising scholarships or part-time jobs, unsafe contact from strangers, oversharing and weak account security. Open conversation at home is the strongest protection.

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

- ⚠ A child or student becomes secretive, anxious or avoids devices after messages.
- ⚠ Contact from a stranger who asks for photos, personal details or to move to another app.
- ⚠ 'Scholarship', 'free gift' or 'job' offers that ask for fees or bank details.
- ⚠ Gaming or in-app purchases made without the family's knowledge.
- ⚠ Elders receiving calls about prizes, KYC or relatives in trouble.

Practical prevention tips

- Talk openly and make it clear that anyone can come to you without fear of blame if something feels wrong.
- Use strong passwords, two-factor authentication and parental or privacy controls that suit the child's age.
- Teach the basics: do not share OTPs, do not click unknown links, do not meet online contacts alone.
- Keep devices and apps updated, and restrict payment methods on children's accounts.
- Help elders set up payment alerts and agree to check with the family before any unusual payment.

Risky habit vs safe habit

RISKY	SAFE
✕ Scold a child for reporting a problem	✓ Stay calm, listen and support
✕ Share passwords with friends	✓ Share them only with parents or guardians
✕ Chat with strangers in online games	✓ Play with friends you know in real life
✕ Hide cyberbullying out of fear or shame	✓ Save the evidence, block and report

What to do if it happens

1. Stay calm and support the person. Do not blame them.
2. Keep screenshots and messages as evidence, then block and report the account on the platform.
3. Report serious harassment or fraud at cybercrime.gov.in and call 1930 for financial fraud.
4. Involve the school or college if the issue involves classmates.

Official reporting resources

- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- 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