Phishing and Fake Websites

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

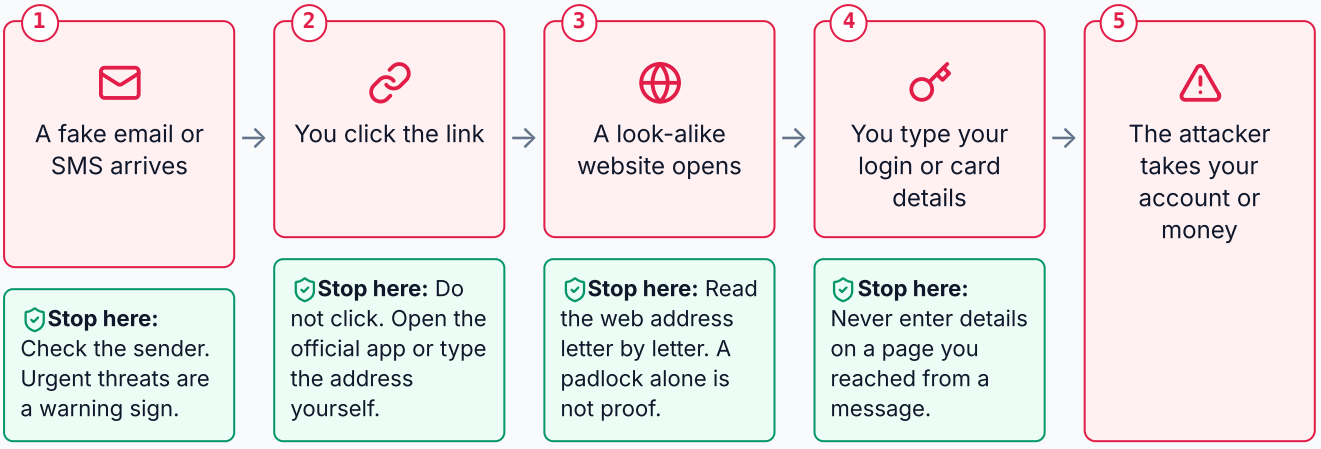
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

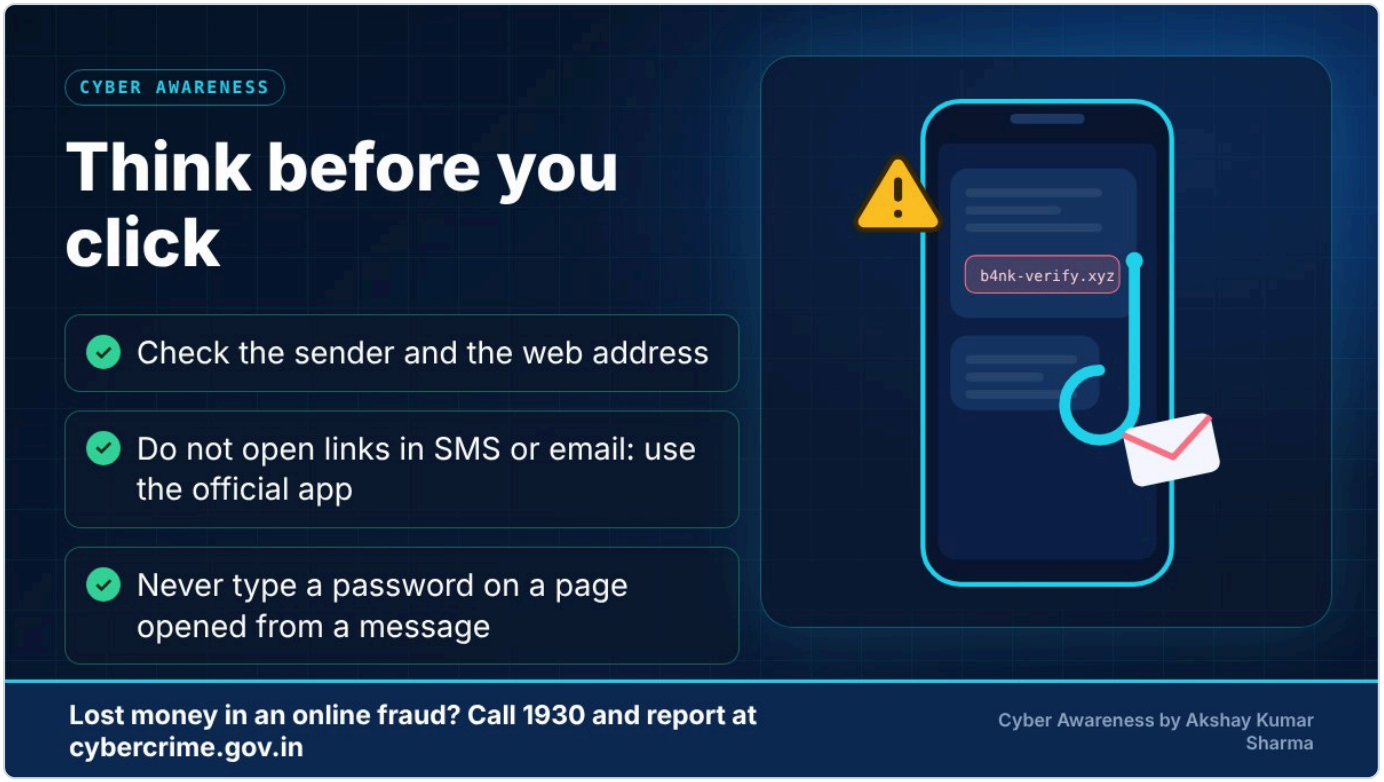
What it is

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