

FREE IDENTITY THEFT PROTECTION GUIDE

10 RED FLAGS YOU SHOULD NOT IGNORE

A fast 2-minute checklist to help you spot suspicious activity before it becomes a bigger problem.

STOP BEFORE YOU CLICK. Fake bank alerts, impersonation messages, suspicious texts, and social-media scams are major tactics consumers are seeing now.

10 IDENTITY-THEFT & SCAM RED FLAGS

1. “Urgent security problem” text from a bank/company. Do not use the link. Open the official app or type the website yourself.
2. A charge, withdrawal, or transfer you do not recognize. Contact the institution using a trusted number and review activity.
3. A one-time passcode you did not request. Change the password and secure the account.
4. Someone tells you to move money to “protect” it. Banks and government agencies do not tell you to transfer money for safekeeping.
5. A notice about an account, loan, or service you never opened. Review your credit reports and contact the company through verified information.
6. Your password stops working or account details suddenly change. Use the provider’s official recovery process and enable multi-factor authentication.
7. Unexpected debt-collection calls or bills. Ask for details and verify whether the account is yours.
8. Mail, statements, or account notifications suddenly stop. Check whether your contact information or mailing address changed.
9. A social-media “friend,” business, celebrity, or support agent asks for money/codes. Verify independently before responding.
10. A message says “Act now,” “You’ll be arrested,” or “Pay immediately.” Urgency is a common scam tactic. Slow down and verify through an official channel.

IF SOMETHING LOOKS WRONG, DO THESE 7 THINGS

1. Pause before clicking links or calling numbers in suspicious messages. 2. Contact the company through a number or website you know is legitimate. 3. Change affected passwords; use a unique password for each important account. 4. Turn on multi-factor authentication.	5. Review bank, card, and credit-report activity for unfamiliar items. 6. Consider a fraud alert or credit freeze if your information may be at risk. 7. Report identity theft at IdentityTheft.gov and follow its recovery steps.
---	--

THE 30-SECOND PROTECTION CHECK

☐ Unique passwords	☐ Multi-factor authentication	☐ Review account alerts
☐ Verify bank contact info	☐ Check credit reports	☐ Know IdentityTheft.gov

SHARE THIS WITH SOMEONE YOU WANT TO PROTECT. | More free resources: RestoreAndHope.info

Educational disclaimer: General educational information only; not legal, financial, cybersecurity, or credit-repair advice. No guarantee of prevention or recovery. For official reporting and recovery guidance, visit IdentityTheft.gov.

Why this matters now: FTC data released in 2026 show imposter scams were the most-reported fraud category in 2025, with \$3.5 billion in reported losses; scams that started on social media accounted for \$2.1 billion in reported losses.