FREE PRACTICE | LIFEREADY

Financial Fraud Warning Signs

Fraudsters may impersonate employers, financial institutions, friends, or officials. They often create urgency and demand an unusual payment or secret information. Verify a claim through independently found official contact information. Do not click, reply, or send a small payment just to investigate.

Worked fictional job offer

'You are hired without an interview. Deposit our check, buy equipment from this link today, and send back the extra money.'

An unexpected check, pressure to return money, and an employer-selected payment route are warning signs. A displayed deposit is not proof that a check is legitimate or finally settled. Stop, involve a trusted adult, and contact the bank through a known channel if money or details were shared.

Identify the warning and safe response

1. A caller claims to be your bank and asks for the code just sent to your phone.

2. A message threatens immediate arrest unless you pay a fine with gift-card codes.

3. A familiar account says a friend urgently needs money but refuses a call. How could you verify safely?

Do not record passwords, real account numbers, identity documents, or contact details here. These are invented educational cases.

© 2026 Penny Hollow. Educational use under the included license.

FINANCIAL FRAUD WARNING SIGNS

Check, explain, and apply

Model responses

- Bank code: do not share it. End the call and use the bank's official app or a known number; the caller may be trying to take over the account.

- Gift-card threat: pressure, impersonation, and an unusual payment method are red flags. Do not pay; verify independently and report the message.

- Friend request: contact the person using a previously known route or speak in person with appropriate support. Their account may have been taken over.

Protect and recover

A free credit freeze restricts access used for new credit and stays until lifted. Contact all three major bureaus. An initial fraud alert lasts one year and can be renewed; contact one bureau to start the alert process across the three. Neither replaces monitoring existing accounts. Minors have a special freeze process.

If information is exposed, contact affected providers through known channels, change exposed credentials, secure accounts with multifactor authentication, and keep records. IdentityTheft.gov offers reporting and a recovery plan. A trusted adult can help a minor take the correct steps.

Your first three steps

1. Write a brief response plan for a fictional exposed password. Include a trusted adult and official recovery route, without private details.

Sources: consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts ; consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams ; IdentityTheft.gov .

Free print license: households and educators may copy this unchanged resource for their own learners. Do not sell, upload as a paid product, or remove Penny Hollow attribution. Keep all practice details fictional; no personal financial information is needed.

© 2026 Penny Hollow. Educational use under the included license.