

Protect Your Retirement Accounts

A 90-minute roundtable on the login, the rollover, and the payment path

Habits

- Do not tap the link. Open the firm's site or app yourself.
- Use a different password for each account. A password manager can hold them. Do not share them.
- Turn on a second factor, such as a code or a fingerprint, on top of the password.
- Install security updates when they arrive.
- Use your own device. Skip a public computer. If you had to use one, clear the history after you log out.
- Wait for a network you trust. Skip cafe and airport Wi-Fi for the account. At home, put a strong password on the router.
- Read the statement when it arrives. Call the firm if money moved, or if the address, email, or phone changed, and you did not do it. A missing statement is a sign too.

Red flags

- A text or email with a link that says the account is locked
- New bank instructions from a messaging app
- A bank or a beneficiary on the statement you did not change
- A missing statement
- Someone who asks you to type a seed phrase into a website, a chat, or a form
- A helper who asks for more crypto to recover crypto that was already sent

First hour

1. **Firm.** Call the firm at the number on the statement, and tell your other firms.
2. **Passwords.** Change the password on that account and on any account that used the same one.
3. **Report.** File at ic3.gov. Identity theft help is IdentityTheft.gov. Investment-account concerns go to FINRA, the SEC, and your state regulator.
4. **Watch.** You can place a fraud alert with the credit bureaus.

Figures on the session page are FBI IC3 2025 totals for those crime types. File a report at ic3.gov.