Immediate Actions to Take if You've Been Scammed:

1. **Contact Your Bank Immediately:**

- Reach out to your bank promptly to report the scam. Inform them of the situation and inquire about freezing or securing your accounts.

2. **Secure Your Online Presence:**

- Change all passwords associated with your accounts. Conduct a thorough check for any unauthorized transactions that may have occurred.

3. **Exercise Caution with Information:**

- Refrain from admitting to the bank that you have unwittingly assisted the scammer. Keep this information confidential for the time being.

4. **Report the Scam:**

- Swiftly report the scam through the official Scamwatch reporting portal at https://www.scamwatch.gov.au/report-a-scam.

Key Steps to Follow:

- **Act Fast to Prevent Further Losses:**

- Take immediate actions to minimize potential financial losses and protect your accounts.

- **Get Help to Recover:**

- Seek assistance from relevant authorities or specialized services to recover any lost funds.

- **Warn Others and Report the Scam:**

- Contribute to the prevention of scams by reporting the incident and warning others about the potential risks.

Watch	Out for	Follow-Up	Scams:
---------	---------	-----------	----------

- Stay vigilant for any follow-up scams that may target you in the aftermath of the initial incident.

- **Get Support in the Aftermath:**

- Seek emotional support or professional advice to cope with the aftermath of the scam and its potential impact on your well-being.

Additional Steps:

- **Report to the Police:**

- File a report with the police and obtain an event number for documentation purposes.

- **Minimize Computer Use:**

- Refrain from using your computer and keep it turned off until instructed otherwise by IT support. This helps prevent further potential security breaches.

Taking these comprehensive steps promptly will contribute to a more effective response to the scam and increase the chances of recovering lost funds.