Crypto Security Checklist

1. Secure Your Wallets

- **Choose Reputable Wallets**: Use well-reviewed and trusted crypto wallets (hardware wallets preferred).
- **Enable Two-Factor Authentication (2FA)**: Add an extra layer of security to your wallet accounts.
- **Backup Your Wallets**: Regularly back up your wallet data and store recovery phrases securely offline.

2. Protect Your Private Keys

- **Keep Private Keys Offline**: Never store private keys in cloud services or on your computer. Use hardware wallets or write them down on paper.
- **Use Strong, Unique Passwords**: Create strong passwords and never reuse them for different accounts.
- **Avoid Sharing Private Keys**: Never share your private keys with anyone.

3. Secure Your Devices

- **Install Antivirus Software**: Protect your devices from malware with reliable antivirus programs.
- **Keep Software Updated**: Regularly update your operating system, apps, and wallets to the latest versions.
- **Use a VPN**: Use a Virtual Private Network (VPN) to encrypt your internet connection and maintain privacy.

4. Be Wary of Phishing Attacks

- **Verify URLs**: Always double-check URLs before logging in to any crypto-related site.
- **Ignore Suspicious Emails**: Do not click links or download attachments from unknown or unsolicited emails.
- **Use Browser Extensions**: Consider using browser extensions that block phishing sites.

5. Conduct Secure Transactions

- **Double-check addresses**: Always verify the recipient's wallet address before sending funds.
- **Use Escrow Services**: For large transactions, consider using a trusted escrow service to protect both parties.

- **Avoid Public Wi-Fi**: Never conduct crypto transactions over unsecured public Wi-Fi networks.

6. Educate Yourself

- **Stay Informed**: Keep up with the latest security practices and news in the crypto world.
- **Learn from Reputable Sources**: Follow advice and updates from trusted crypto experts and communities.

7. Regular Audits

- **Review Security Regularly**: Periodically review and update your security measures.
- **Monitor Accounts**: Regularly check your accounts for any unauthorized transactions or access.

8. Emergency Plan

- **Have a Recovery Plan**: Know the steps to take if your accounts are compromised.
- **Contact Support Immediately**: Have wallet and exchange support team contact information handy.