Checklist: How to stay safe when using cryptocurrency exchanges

1. **Use Cold Wallets for Long-Term Storage**
   - Only keep the funds you need for immediate trading on the exchange.
   - Store the rest offline in a cold wallet to protect against internet-based threats.

2. **Activate Two-Factor Authentication (2FA)**
   - Enable 2FA with an app like Google Authenticator to add an extra security layer to your account.

3. **Double-Check URLs**
   - Always type the exchange URL directly into your browser rather than clicking links in emails or ads.
   - Verify that the URL is correct to avoid phishing sites.

4. **Use Strong, Unique Passwords**
   - Create a complex, unique password for your exchange account that includes numbers, symbols, and a mix of upper and lowercase letters.
   - Avoid reusing passwords across multiple sites.

5. **Beware of Phishing Scams**
   - Watch for suspicious emails or messages asking for personal information or login details.
   - Always verify the source of any message before taking action.

6. **Keep Your Software Up-to-Date**
   - Regularly update your operating system, browser, and antivirus software to protect against security vulnerabilities.

7. **Avoid Public Wi-Fi for Trading**
   - Use a secure, private internet connection when accessing your exchange account, as public networks are more vulnerable to attacks.

8. **Monitor Account Activity Regularly**
   - Check your account history frequently for any unauthorized transactions.
   - Set up alerts, if available, for any activity on your account.

9. **Use Hardware Authentication Keys (if supported)**
   - Some exchanges support hardware authentication keys, like YubiKey, for even stronger 2FA.

10. **Withdraw Your Earnings Regularly**
    - Don’t leave profits sitting on the exchange; withdraw funds to a secure wallet when you’re not actively trading.

KRYPTOTECK