DeFi Security Audit Checklist

Professional Risk Assessment

Protocol Due Diligence

Before investing in any DeFi protocol, com

[ ] Smart Contract Audits

- Check for audits by reputable firms:
  * Trail of Bits, Consensys Diligence, C
  * CertiK, Quantstamp, PeckShield
- Review audit reports for critical/high s
- Verify audits are recent (within 6 mont

[ ] Protocol Track Record

- Time in production: Minimum 6 month
- Total Value Locked (TVL): Higher gen
- History of exploits or bugs: Check pas
- Bug bounty program: Active program

[ ] Team and Governance

- Team transparency: Known vs anonyn
- GitHub activity: Regular commits and
- Community engagement: Active Disco
- Governance model: Decentralization l

[ ] Smart Contract Analysis

- Code is open source and verified on E
- Admin keys and upgrade mechanisms
- Timelock on sensitive functions (24-48
- Multi-sig requirements for critical oper

Wallet Security Best Pra

[ ] Hardware Wallet Usage

- Use Ledger or Trezor for significant ho
- Never share seed phrase or private ke
- Store seed phrase physically in secur
- Consider multi-location backup strateg

Transaction Security Checklist

[ ] Pre-Transaction Verification

- Double-check recipient address
- Verify contract address on official documentation
- Review transaction details in wallet before signing
- Check gas fees are reasonable for network conditions
- Use simulation tools (Tenderly, Blocknative)

[ ] Token Approval Management

- Only approve necessary token amounts
- Revoke unlimited approvals after transactions
- Regularly audit approvals using Etherscan or Revoke.cash
- Never approve untrusted or new contracts

Ongoing Monitoring and Maintenance

[ ] Position Monitoring

- Set price alerts for liquidation levels
- Monitor collateralization ratios daily
- Track protocol TVL and stability
- Watch for governance proposals affecting positions

[ ] Security Tools to Use

- DeFi Safety: Protocol safety ratings
- Revoke.cash: Manage token approvals
- Etherscan: Verify contracts and transactions
- MetaMask transaction insights
- Wallet Guard: Phishing protection

Red Flags to Avoid

NEVER invest in protocols with these characteristics:

X No smart contract audit from reputable firm
X Anonymous team with no track record
X Unrealistic APY promises (>1000%)
X Closed-source or unverified contracts
X Less than $1M TVL for new protocols
X Heavy marketing focus with little technical detail
X Copying code from other projects without audit
X Centralized control without transparency

Emergency Response Plan

If you suspect a security breach:

1. Immediately move funds to secure wallet
2. Revoke all token approvals for affected contracts
3. Document all transactions and evidence