

# [ PDF Database Document ] - BTCC Cryptocurrency Exchange

원문:

<https://www.btcc.com/ko-KR/academy/research-analysis/how-to-keep-your-cryptocurrency-wallet-safe-from-hackers>

## 해커로부터 암호화폐 지갑을 안전하게 유지하는 방법?

암호화폐의 인기가 높아지고 있는 동시에 위협도 진화하고 성장하고 있습니다. 점점 더 많은 사람들이 암호화폐에 투자함에 따라 공격자에게 점점 더 유리해집니다. 최근 암호화폐 도난 피해자 중 한 명이 솔라나 블록체인 기반 [암호화폐 지갑](#)(cryptocurrency wallet)이었습니다. 가장 인기 있는 솔라나 지갑 중 일부는 해킹으로 인해 타격을 받았습니다.

암호화폐 거래소와 지갑이 안전하지 않다면 암호화폐 거래를 중단해야 하나요? 물론 그것도 좋은 방법인데 해커로부터 보호하는 것도 좋습니다. 그에 대해 무엇을 할 수 있는지 조금 더 자세히 알아보겠습니다.

관련페이지:

[솔라나\(SOL\)해킹 발생, 300만달러 손실…국내 거래소 입출금 중단 - BTCC](#)

[솔라나 CEO “솔라나 해킹, 슬로프 지갑과 연관 가능성 있다” - BTCC](#)

## 1. 콜드 월렛 사용

암호 지갑에는 두 가지 유형이 있습니다.

핫월렛 - Exodus 및 MetaMask와 같은 인터넷에 연결된 지갑입니다.

콜드 지갑 - 오프라인 지갑으로, USB 장치와 같이 인터넷에 연결되지 않습니다.

핫 월렛은 언제 어디서나 로그인할 수 있지만 데이터 도난 및 침해 위험이 더 큽니다. 콜드 월렛을 설정하려면 약간의 기술 지식이 필요하며 더 안전한 것으로 간주됩니다. 그러나 오프라인 지갑을 분실한 경우 복구할 수 있는 “비밀번호 찾기” 옵션이 없습니다.

가능한 최고 수준의 보안을 갖춘 하드웨어 지갑 개발자인 Ledger가 좋은 예입니다. 암호화 통화의 개인 키는 정교한 보안 조치와 함께 제공되는 USB 스틱에 여러 보안 계층에 저장됩니다.

## 2. 비밀번호 강화 및 장기전 변경

한 연구에 따르면 MZ세대의 75%가 여러 기기에서 동일한 비밀번호를 사용합니다. 그리고 깨는데 얼마나 걸립니까? 글쎄, 거의 1초뿐입니다!

따라서 비밀번호를 보호하는 핵심은 복잡한 비밀번호를 설정하고 안전하게 보관하고 자주 변경하는 것입니다. 암호화폐 지갑이나 기타 민감한 사이트의 비밀번호를 선택할 때 이미 가지고 있는 비밀번호를 재사용하지 마십시오. 또한 비밀번호에는 개인 정보가 포함되어서는 안 됩니다.

브라우저에 비밀번호를 저장하는 대신 LastPass 또는 1Password와 같은 비밀번호 관리자에 비밀번호를 저장하는 것이 더 안전합니다. 마지막으로 약 6개월마다 비밀번호를 변경하는 것이 추천합니다.

### 3. 개인 키는 항상 자신에게 보관

개인 키의 교환은 절대 있어서는 안 됩니다. 개인 키 사본을 얻은 사람은 누구나 모든 디지털 자산을 완벽하게 제어할 수 있습니다. 개인 키는 안전한 위치에 보관하고 자주 변경하여 보호할 수 있습니다. 구글 또는 메타(전 페이스북)과 같은 여러 로그인에서 동일한 개인 키(비밀번호)를 사용하지 마십시오. 개인 키를 항상 컴퓨터와 모바일 장치의 손이 닿지 않는 곳에 두십시오. 그것을 기록하고 당신만이 당신의 키에 접근할 수 있는 장소에 보관하는 것이 그것을 추적하는 가장 좋은 방법입니다.

### 4. 피싱 조심

피싱은 공격자가 귀하의 민감한 정보를 획득하기 위해 합법적인 주체로 가장할 수 있는 표적 공격이며, 사람들이 얼마나 자주 이에 속아 넘어가는지 알 수 있습니다. 피싱을 방지하려면 올바른 사이트에 있다고 확신하지 않는 한 암호화폐 거래소에 로그인하면 안됩니다. 다른 사람이 임의로 보낸 링크를 클릭하지 말고 즐겨찾기에 대한 링크를 저장하거나 URL을 입력합니다. 또한 개인 정보를 요구하는 문자, 이메일 또는 채팅을 신뢰하지 않습니다.

마지막으로, 지불을 보내기 전에 항상 세부 정보가 정확한지 다시 한 번 확인해야 합니다.

### 5. 암호화폐와 개인/업무 분리

개인 및 업무 장치 및 계정에서 암호화폐 거래를 분리하는 것이 권장합니다. 액세스 권한을 잃을 수 있는 개인, 학교 또는 직장 이메일을 사용하는 대신 암호화 지갑 전용 이메일을 만들어야 합니다. 직장이나 공용 컴퓨터에서 암호 지갑에 액세스하지 말고 전용 노트북이나 스마트폰과 같은 암호 거래를 위한 별도의 장치를 사용하는 것을 고려해야 합니다.

### 6. 공용 Wi-Fi 네트워크에 연결하지 않음

공용 WiFi를 사용하여 온라인 암호화 지갑이나 거래소에 액세스하지 마십시오. 다른 옵션이 없으면 VPN(가상 사설망)을 사용하여 위치와 IP 주소를 마스킹하십시오. VPN(가상 사설망)은 실제 위치와 IP 주소를 숨기므로 모든 온라인 활동을 익명으로 수행할 수 있습니다.

### 7. 평판이 좋은 거래소를 사용하여 매입/매도

거래를 하기 전에 일부 거래소는 다른 거래소보다 더 안전하다는 점을 이해해야 합니다. 과거에 어떤 암호화폐 거래소가 손상되었는지 알아보기 위해 조사를 합니다. 거래소가 해킹되면 보안 관행이 좋지 않거나 기존 취약점이 나타나 투자가 위험할 수 있기 때문입니다.

대부분 암호화폐 거래소는 사이버 공격 시 암호화폐 투자를 법적으로 보장할 수 없기 때문에 해킹을 당하면 자산을 잃을 수 있습니다. 손실을 줄이기 위해 계정을 동결할 수 있는 옵션이 있는지 확인하십시오.

---

**BTCC거래소**는 2011년에 설립된 암호화폐 선물거래소이며 현재 까지 세계 최장 운영되고 있습니다. **해킹 피해 사례가 없는** 강력한 보안을 자랑해 투자자가 보다 더 안전하게 거래할 수 있는 환경을 제공하고 있습니다.

BTCC는 전 세계 모든 암호화폐 애호가들에게 공정한 거래 분위기를 조성하기 위해 거래의 모든 측면을 개선하는 데 많은 노력을 기울여 왔습니다.

현재 코인체코의 선물 거래소 순위 5위이며, 전 세계 130개국, 수백만 가입자들에게 29개 페어의 암호화폐 선물 거래 서비스를 제공하는 [프리미엄](#) 블록체인 자산 거래 및 투자 서비스를 제공합니다.

BTCC거래소는 [미국 금융감독국\(MSB\)](#), [캐나다 금융감독국\(MSB\)](#)의 라이센스에 이어 새롭게 리투아니아의 암호화폐 라이센스를 획득했습니다. 이로써 BTCC는 유럽의 규제하에 암호화폐 거래소 운영하도록 엄격히 규제를 받습니다.

관련페이지:

[암호화폐 지갑이란? 비트코인 지갑은? 초보자 위한 가이드 - BTCC](#)

[비트코인 지갑에 대한 알아야 하는 것 - BTCC](#)