

장치 암호화(Bitlocker) 해제 방법

BitLocker는 드라이브를 암호화하여 데이터를 보호하는 Windows 보안 기능입니다.
이 암호화는 누군가가 오프라인으로 디스크에 액세스하려고 하면 해당 콘텐츠를 읽을 수 없도록 합니다.

BitLocker는 중요한 정보를 안전하게 유지하므로 디바이스를 분실하거나 도난당한 경우에 특히 유용합니다.
사용자에게 친숙하도록 설계되었으며 Windows 운영 체제와 원활하게 통합되어 쉽게 설정하고 관리할 수 있습니다.

BitLocker 기능이 설정되어 있는 상태에서 TPM 초기화, BIOS 업데이트, 하드웨어 교체 등의 작업이 진행될 경우 복구 키를 요구할 수 있습니다.
또한, Windows 대형 업데이트등으로 인해 TPM 관련 업데이트 등이 진행될 경우에도 복구 키를 요구할 수 있습니다.
※ BIOS를 업데이트 하기 전 장치 암호화를 해제하지 않으면 재부팅 후 장치 암호화 키를 인식하지 못하여, 재부팅할 때마다 복구 키를 입력하라는 메시지가 표시될 수 있습니다.

복구 키는 장치 암호화 (BitLocker)를 설정할 때 생성되며, Microsoft 계정에 저장이 됩니다.
복구 키를 분실했다면 스마트폰이나 주변의 다른 PC를 이용하여 MS BitLocker 복구 키 사이트에 접속하여 해당 키를 입력할 경우 해제할 수 있습니다.

장치 암호화는 다음의 조건에서 자동 활성화 됩니다. (Windows 11/ 10 Home 버전 기준)

- ① Modern Standby 적용 제품
- ② Microsoft 계정 사용
- ③ BIOS에서 TPM 기능 On 상태
- ④ BIOS에서 Secure Boot 기능 On 상태

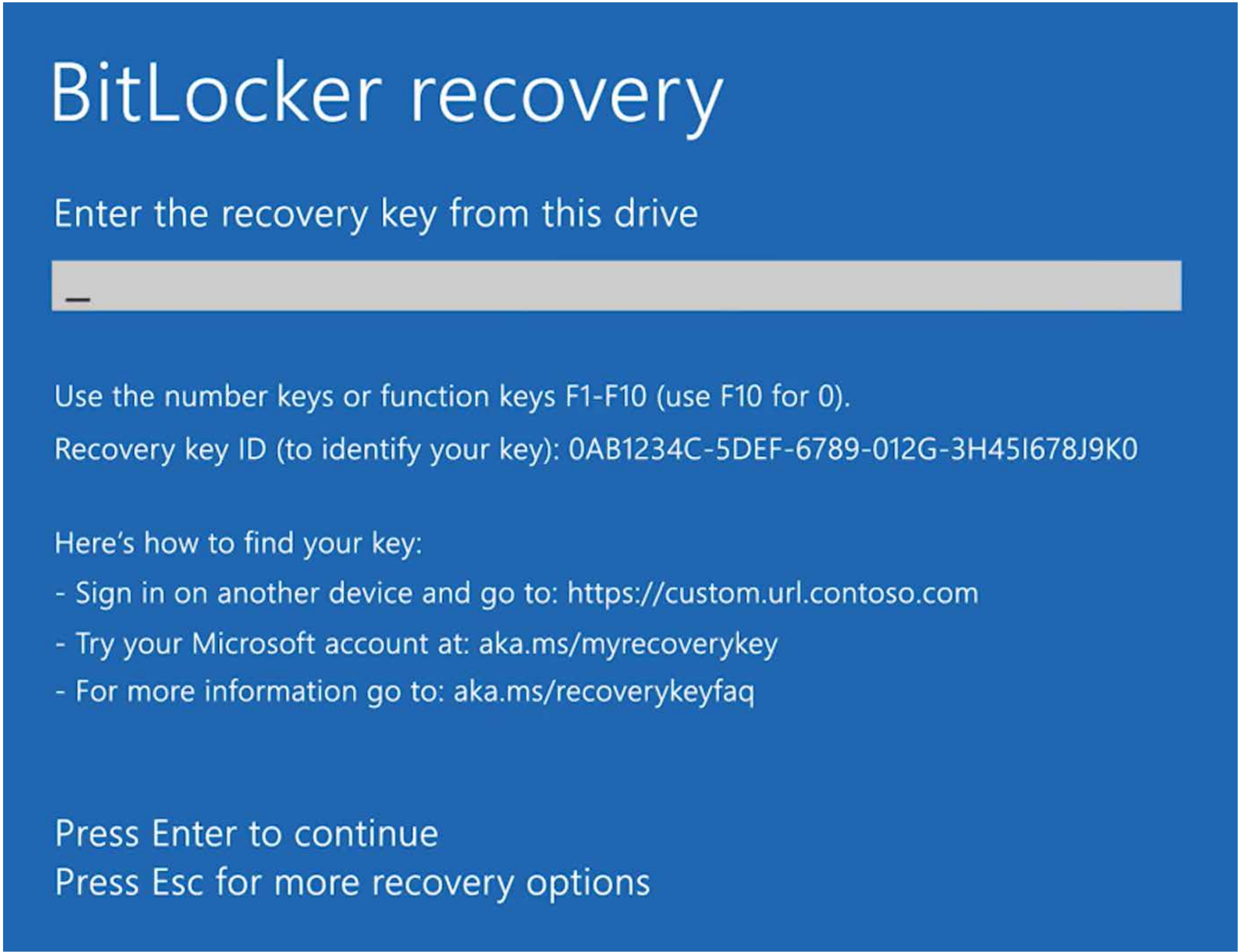
1. 장치 암호화 해제(끄기 방법)

*다만, 장치 암호화 (Bitlocker) 를 해제할 경우 Microsoft Copilot 기능의 일부 기능 (Recall 등)을 사용할 수 없습니다.

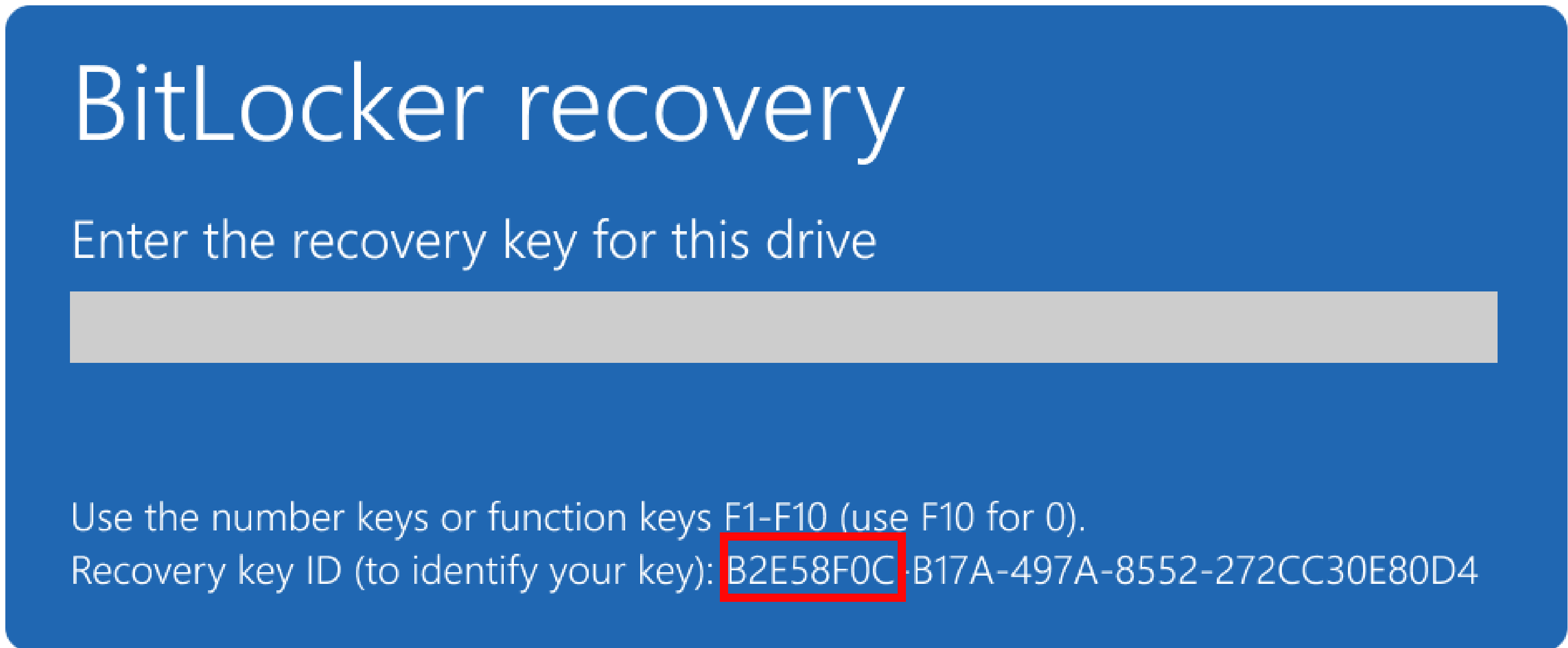
- 1) Windows 로고 키 + i를 누른 후 Windows 설정을 실행합니다.
- 2) 개인 정보 및 보안 항목에서 '장치 암호화'로 진입합니다.
- 3) '장치 암호화' 옵션을 '끔' 으로 설정합니다.
- 4) [장치 암호화를 끄시겠습니까?] 창이 표시되면 [끄기]를 선택합니다.
- 5) 장치 암호화 해독이 진행되면서 암호화 해제가 진행되며, 데이터가 많은 경우 시간이 다소 소요될 수 있습니다.

2. 장치 암호화가 활성화 된 경우

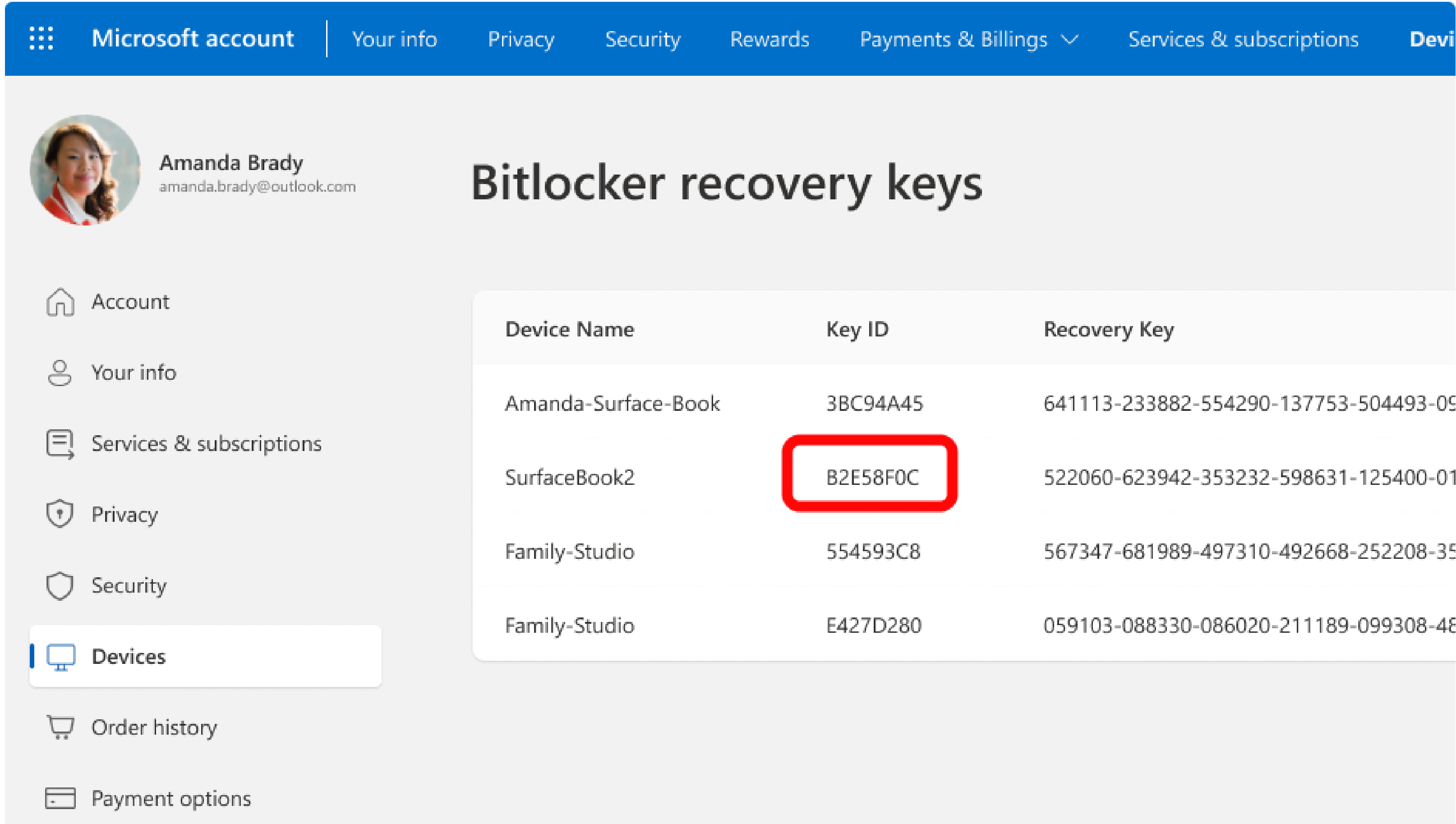
* 제품 시동 과정에서 아래와 같은 EFI 화면이 표시되며, 이 과정에서 CPU가 100%로 동작하기 때문에 발열이 발생할 수 있습니다.



- 1) 복구 키를 입력하라는 메시지가 표시되면 복구 키 ID의 처음 8자리를 기록해 둡니다.



- 2) 다른 디바이스에서 웹 브라우저를 열고 <https://aka.ms/myrecoverykey> 에 접속합니다.
- 3) 제품에 로그인하였던 Microsoft 계정으로 로그인 후 1) 에 기록하였던 키 ID를 찾습니다.
- 4) 해당 키 ID에 기재된 복구 키를 사용하여 드라이브 잠금을 해제합니다.



만약, 복구 키를 분실한 경우 데이터를 복원할 수 없으며, 드라이브를 포맷해야만 사용할 수 있습니다.
이 과정에서 모든 파일이 제거되며, 이와 관련해서는 TUVA를 포함하여 Khadas 또한 도움을 드릴 수 있는 것이 없습니다.
복구 키는 계정에 귀속되기 때문에 기능을 개발한 Microsoft에서도 복구 키를 제공하거나 다시 만들 수 없습니다.