사이버 보안의 종류 5가지에 대하여 나열하고, 그에 대하여 간략하게 서술하시오.

1. **디지털 흔적 분석하기:** 디지털 분석은 매우 방대해서 전부 삭제가 불가능 합니다. 온라인 전역에 정보가 퍼지기 때문에 가치 있는 정보가 어떤 사이트에 저장돼 있는지 파악하는게 중요하다. 이용하지 않은 사이트가 있다면, 해당 사이트의 사용자 계정을 삭제한다.
2. **가장 민감한 계정의 우선순위 정하기:** 사용자는 개인 자산 정보와 개인 건강 정보와 같은 민감한 데이터를 조유하고 있는 계정에 우선순위를 둘 수 있다. 좀 더 쉽게 하기 위해서는 각각의 사이트와 관련된 데이터 민감도에 따라 보안 수준을 낮음/중간/높음으로 분류하면 된다 그리고 얼마나 많은 문제가 발생할 수 있는지도 고려해야 한다. 누군가가 사용자 계정을 해킹해서 얻은 정보로 데이터 수정이나 부당 요금 청구, 신원 도용과 같은 문제를 일으킬 수 있다.
3. **우선순위가 높은 계정에는 가능한 강한 접근 제어와 인증 방식 설정하기:** 우선순위가 높은 계정에는 좀 더 강력한 비밀번호를 설정하거나 보안 질문을 변경하는게 좋다. 혹은 계정의 비밀번호를 자주 바꾸는 것도 한 방법이다. 가능하다면 사용자는 온라인 뱅킹, 아이클라우드와 같은 모바일 앱에 2단계 인증를 설정하는 것이 좋다.
4. **보안 패치를 최신 상태로 유지하기, 온라인에 정보를 제출 할 때 주의하기, 데이터를 주기적으로 백업하기:** 바이러스, 악성 코드의 위협을 최소화하기 위해서는 운영체제, 브라우저와 같은 소프트웨어에 대한 최신의 보안 패치를 받아야 한다. 게시물을 작성할 때는 최소한의 개인 정보만 담아야 한다. 그리고 온라인 서비스 또는 외장 디바이스에 자신의 데이터를 백업 해야 한다. 자동 백업 스케줄은 규칙적인 데이터 백업의 한 방법이 될 수 있다.
5. **자신만의 BC/DR 계획 미리 갖추기:** 의심스러운 행위를 탐지하기 위해서는 사용자 계정을 늘 예의 주시해야 한다. 단순히 은행 계좌뿐만 아니라, 사용하지 않은 국제전화 비용이 직불 카드에서 작동 이체로 빠져나가는 해킹이 일어날 수 이는 다른 온라인 서비스도 살펴봐야 한다. 사용자는 자신만을 위한 비즈니스 연속성 (BC)/재해 복구 (DR) 계획을 세운다면 데이터가 물리적 손상을 입는 경우나 사용자 계정이 사이버 공격으로 침해 당한 경우에 대비하는 데 도움이 된다. 신분 도용을 신고 할 수 있는 전화번호 목록과 도난을 대비해 신용 카드 번호 목록은 따로 보관해준다.