Homeland Security

국토안보부
파트너십 및 참여 사무소(OPE)

독싱(신상털기) 위협에 처한 개인을 위한 리소스

2024년 1월 16일

독싱이란 무엇인가?

독싱은 공개적인 수치심, 스토킹, 신원 도용, 괴롭힘의 표적화 등 악의적인 목적으로 개인의 개인 식별 정보를 수집하여 공개적으로 공개하는 행위를 말합니다.

민감한 정보의 예

- 전체 이름
- 연락처 정보
- 집 주소
- 가족 구성원
- 직장 세부 정보
- 재무 정보
- 사회 보장 번호

민감한 정보의 일반적인 출처

- 소셜 미디어 게시물
- 부동산 및 법원 기록
- 결혼식 공지 및 부고
- 뉴스레터
- 공개 회의
- 웹 포럼, 블로그 및 토론 게시판
- 보호되지 않는 네트워크
- 유권자 등록 목록

독싱으로부터 자신을 보호하려면 어떻게 해야 하나요?

- 일시적인 경우라도 사진과 동영상을 포함하여 자신에 대한 정보를 온라인에 게시할 때는 **주의하세요.**
- 소셜 미디어 프로필에서 PII(주소, 생년월일, 휴대폰 번호 등)를 **삭제합니다.**
- 팔로워를 **검토하고** 모르는 사람의 요청을 거절하세요.
- 공공 기록 웹사이트에서 개인 데이터 삭제 **요청하기.** 잘 알려진 웹사이트로는 BeenVerified, FastPeopleSearch, 인텔리우스, 피플파인더스, 스포코, 트루스파인더, 화이트페이지 등이 있습니다.
- 불필요한 앱과 브라우저 확장 프로그램을 **제거하여** 개인 데이터 수집을 방지하세요.
- 앱과 웹사이트에서 위치 추적을 **제한합니다.** 각 앱 또는 플랫폼의 위치 서비스를 끕니다.
- 소셜 미디어, 앱, 기타 웹사이트의 개인정보 보호 설정을 **켭니다.**
- 2단계 인증을 **설정하고**, 복잡한 비밀번호를 사용하며, 여러 계정에 동일한 비밀번호를 반복해서 사용하지 마세요.

DHS OPE

독싱으로부터 자신을 보호하려면 어떻게 해야 하나요?

허위, 모욕적 또는 위협적인 콘텐츠 삭제 요청
규칙 및 요구 사항에 따라 플랫폼 또는 웹사이트에 게시 중단 요청을 제출하는 것이 좋습니다.

진행 상황을 문서화
증거를 보존하기 위한 조치를 취하는 것이 좋습니다. 수신한 모든 이메일, 음성 메일, 문자 메시지를 저장하고 소셜 미디어에 올라온 댓글의 스크린샷이나 사진을 찍어 보관합니다.

사건 신고하기
신체적 안전에 위협을 받거나 범죄적 괴롭힘을 당했다고 생각되면 현지 법 집행 기관과 소셜 미디어 플랫폼 또는 웹사이트 관리자에게 사건을 신고하세요.

추가 리소스 및 안내

CISA 사이버 보안 모범 사례 및 리소스: cisa.gov/cybersecurity
CISA 사이버 에센셜: cisa.gov/cyber-essentials
CISA 팁: 소셜 엔지니어링 및 피싱 공격 방지: cisa.gov/tips/st04-014
CISA 인사이트: 이메일 및 웹 보안 강화: cisa.gov/publication/enhance-이메일-및-웹-보안-강화
교직원 및 당국을 위한 CISA 소셜 미디어 위협 지침 인포그래픽: https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic
온라인 범죄의 피해자인 경우, ic3.gov에서 **FBI의 인터넷 범죄 신고 센터(IC3)에** 신고하세요.