Ready HoCo
choose preparedness

Calvin Ball
County Executive

사이버보안

사이버공격은 컴퓨터나 네트워크 시스템에 접근하거나 그에 손상을 주려고 하는 나쁜 행위입니다. 사이버공격으로 돈을 뺏기도 하고, 인적 정보, 재무 정보, 의료 정보를 빼가기도 합니다. 사이버공격으로 사람의 명성과 안전에 피해를 줄 수도 있습니다.

사이버보안은 사람, 조직, 지역사회, 국가 등에 광범위한 영향을 줄 수 있는 사이버공격을 예방하고, 탐지하고, 대응하는 활동입니다.

미리다음과같은조치를취하여 사이버위험을피할수있습니다:

- 공유하는 온라인 정보의 제한. 프라이버시(개인정보보호) 설정 변경 및 위치 추적 기능 불사용.
- 소프트웨어 프로그램과 운영시스템을 최신으로 유지.
- 대문자, 소문자, 숫자, 특수문자 등을 사용하여 강력한 비밀번호 생성. 비밀번호 관리프로그램 및 두 가지의 인증방법 사용.
- 즉시 무엇을 할 것을 요구하거나, 너무 좋아서 사실이라고 보기 어려운 것을 제안하거나, 개인정보를 필요로 하는 의심스러운 상황에 유의. 클릭하기 전에 생각. 의심스러울 경우에는 클릭하지 말 것.
- 은행 계좌번호, 사회보장번호(SSN), 신용카드 번호 등과 같은 개인 재무 정보를 공유하는 것에 유의. https:// 로 시작되는 보안이 설정된 사이트에서만 개인 정보 공유. 유효하지 않은 인증이 포함된 사이트의 이용 금지. 보안이 조금 더 확보되는 연결망을 가진 가상 사설망(VPN)의 이용.
- 모르는 사람으로부터 온 문자나 이메일의 링크 클릭 금지. 스캐머(사기꾼)는 가짜 웹사이트 링크를 만듭니다.

사이버공격이진행되는동안

- 인정할 수 없는 과금에 대해 신용카드와 은행 거래내역을 확인하십시오.
- 자신이 개설하지 않은 신규 계좌나 융자가 있지나 않은지 신용보고서를 확인합니다.
- 사적 정보를 묻는 이메일과 소셜미디어 사용자를 조심하십시오.
- 수상한 활동이 느껴지면, 즉시 모든 인터넷 계정 비밀번호를 바꾸어서 피해를 최소화합니다.
- 직장이나 학교, 기타 시스템 운영자가 어떤 일이 일어났는지 알게 하십시오.

사이버공격이끝난후

- 본인의 계좌가 있는 은행, 신용카드 회사, 기타 재무 서비스 기관에 연락합니다. 공격을 받은 계좌를 정지시켜야 할 수 있습니다. 허락받지 않은 신용계좌나 과금 계정을 닫습니다. 누군가가 자신의 신분을 사용하고 있을 수 있다는 것을 신고합니다.

- 누군가가 자신의 사회보장번호를 불법적으로 사용하고 있다고 생각되면, 감찰국(OIG)에 신고합니다.

- 연방거래위원회(Federal Trade Commission)에 신원도용을 신고합니다. 정부 요원이라고 칭하는 사람으로부터 메시지를 받았다ftc.gov/complaint에서 연방거래위원회(FTC)에 알리십시오.

- 어떤 정보를 도난 당했는가에 따라 다른 기관에 연락해야 할 수도 있습니다.