현명한 사이버 사용자가 되세요: “방비책 사용”이 필요합니다

온라인 안전을 위한 간단한 수칙

사이버 사기는 새로운 사실이 아닙니다. 매일 해커들과 사이버 범죄자들은 온라인 상에서 쉬운 표적을 찾고 있습니다. 본인은 온라인 약탈자들의 표적이 될 것 같지 않으시다고요? 다시 한번 생각해 보세요!

당신의 개인 신분 정보, 은행 정보, 혹은 단순히 당신의 이메일 안에 들어있는 어떠한 내용이라든지, 당신의 모든 정보는 중요하며 사이버 범죄자들은 그 정보를 얻기 위해 온갖 수단을 동원할 것입니다. 당신 본인은 표적이 되지 않을 것이라고 생각하는 점을 그들은 악용합니다. ***방비책 사용*** 을 하여 사이버 범죄의 피해자가 되는 것을 미연에 방지할 수 있는 수칙을 실천할 때입니다.

사이버 위생의 기본 수칙부터 시작해 봅시다. — 쉬운 상식적 방법으로 온라인에서 스스로를 보호하세요. 여기 네 가지 방법을 오늘부터 실천하여 사이버 안전을 지킵시다:

- **모든 온라인 계좌에 다수의 인증 방법을 사용하세요.** 비밀 번호만으로는 온라인에서 당신의 안전을 지킬 수 없습니다. 문자 메시지 승인, 본인 확인 앱으로부터 암호 수신, 얼굴 혹은 지문 식별 확인, 또는 보안 키를 활용하여 신원 확인 방법을 이중막으로 설정함으로써, 당신이 로그인 하는 은행, 이메일 공급자, 혹은 여타 인터넷 사이트에 추가 보안 보호막을 제공하게 되는 것입니다. 다요소 인증 방법을 쓰면 해킹 당하거나 개인 정보가 도난 당할 수 있는 가능성을 99 퍼센트까지 줄일 수 있습니다!
- **소프트웨어를 최신화 하세요.** 해커들은 소프트웨어의 결함과 약점을 부당 활용하려고 합니다. 핸드폰, 태블릿, 노트북 컴퓨터 같은 당신이 사용하는 모든 기기의 시스템 소프트웨어를 최신화 하세요. 또한 응용 프로그램 – 특히 웹 브라우저 - 도 꼭 정기적으로 최신화 하세요. 모든 기기, 앱, 운영 체계의 자동 업데이트 선택을 단순히 켜 놓는 것 만으로도 쉽게 해결할 수 있습니다.
- **클릭하기 전에 한번 더 생각하세요.** 90 퍼센트 이상의 사이버 공격이 피싱 이메일로 오는 낯선 링크를 클릭함으로써 발생합니다. 피싱 음모는, 그 링크 혹은 웹사이트를 합법적인 것처럼 보이게 하지만, 당신의 비밀 번호, 신용카드 번호, 혹은 다른 민감한 정보를 노출시키게끔 유도하려고 만들어진 속임수일 뿐입니다. 덧붙여, 피싱 이메일은

악성 코드라 불리우는 악의적인 소프트웨어를 사용하게끔 유인하는 시도입니다. 당신이 잘 모르는 링크라면, 당신의 직감을 믿으시고 클릭 하시기 전에 한번 더 생각하세요.

- **견고한 비밀 번호를 사용하세요.** 견고한 비밀 번호는 적어도 8 개 이상의 문자, 숫자, 특수문자의 조합입니다. 여러 다른 웹사이트에서 같은 비밀번호를 사용하는 것을 피하세요. 이상적인 방법은, 비밀 번호 관리 프로그램을 사용하여 특이한 비밀 번호를 생성시키고 보관하는 것입니다.

현 시대에서의 디지털과 상호 연결은 증가 일로에 있습니다. 우리는 우리 모두가 의존하는 컴퓨터 통신망을 제대로 보호하는 데에 각자의 책임이 있습니다. 사이버 보안의 옹호자가 되어서 이러한 정보를 친구, 가족, 이웃들과 나눠 주세요.

추가 정보를 원하신다면, CISA 의 "방비책 사용" 웹페이지 를 방문해 주세요.