온라인 보안 및 사기 예방: 전자 디지털 시대에 자신을 보호하는 방법

인터넷은 우리가 말하고, 쇼핑하고, 사업을 수행하는 방식에 혁명을 일으켰지만, 사이버 보안 위험과 온라인 사기도 증가시켰습니다. 사이버 범죄자와 사기꾼이 지속적으로 기술을 향상시키면서, 온라인 보안과 사기 감소를 이해하는 것은 개인 및 경제적 정보를 보호하는 데 필수적입니다. 먹튀검증 인터넷을 탐색하는 사람이든 소비자 정보를 관리하는 기업이든, 행동 조치를 취하면 사이버 범죄에 피해자를 떨어뜨릴 가능성을 크게 줄일 수 있습니다.

온라인 위험 이해

사이버 범죄자들은 피싱 공격, 스파이웨어 및 애드웨어 공격, 신원 도용, 경제적 사기를 포함한 취약점을 이용하기 위해 다양한 기술을 사용합니다. 피싱 사기는 사기성 이메일 메시지, 이메일 또는 아마도 사람들이 비밀번호나 소비자 은행 정보와 같은 매우 민감한 세부 정보를 공개하도록 직접 유도하는 사이트를 수반합니다. 파괴적인 컴퓨터 소프트웨어와 유사한 스파이웨어와 애드웨어는 위험한 검색이나 의심스러운 백링크를 통해 기기를 쉽게 오염시켜 사이버 범죄자가 정보를 가져가거나 신체를 제어할 수 있도록 합니다. 사기꾼이 개인 정보에 액세스하여 신용 잔액을 시작하거나 무단 인수를 만드는 것과 같은 사기를 저지르는 데 사용할 때마다 ID 도난이 발생합니다.

온라인 보안을 위한 중요한 방법

강력한 비밀번호 사용 - 견고한 코드는 최소 12자 이상이어야 하며 대문자, 소문자, 숫자 및 특정 상징이 포함되어야 합니다. 생일이나 자주 사용하는 단어와 같이 쉽게 추측할 수 있는 비밀번호는 사용하지 마십시오. 복잡한 비밀번호를 안전하고 보안되게 보관할 수 있도록 코드 디렉터를 고용하는 것을 고려하세요.

2단계 인증(2FA) 허용 - 예를 들어 휴대전화로 전송되는 확인 프로그램 코드와 같은 보안에 대한 보완 수준을 통합하면 사이버 범죄자가 코드를 받더라도 잔액에 액세스하는 것을 훨씬 더 어렵게 만듭니다.

컴퓨터 소프트웨어 및 가젯을 최신 상태로 유지 - 운영 체제, 브라우저 및 보안 소프트웨어를 정기적으로 변경하면 사이버 범죄자가 사용할 수 있는 취약점을 복구하는 데 도움이 됩니다. 프로그래밍된 개정을 통해 최신 방어책이 있는지 확인하세요.

이메일 메시지 및 백링크에 주의하세요 - 피싱 사기는 일반적으로 금융 기관, 소셜 미디어 마케팅 프로그램 또는 온라인 소매업체에서 온 평판이 좋은 마케팅 및 영업 커뮤니케이션으로 가짜 이메일을 위장합니다. 의심스러운 백링크를 선택하거나 알 수 없는 옵션에서 첨부 파일을 다운로드하지 마세요.

인터넷 관계 보호 - 사이버 범죄자가 보장되지 않은 사이트에 대한 정보를 쉽게 가로챌 수 있으므로 민감한 구매와 관련하여 커뮤니티 Wi-Fi를 사용하지 마십시오. 공공 장소에서 인터넷을 볼 수 있는 경우 VPN(전자 전용 커뮤니티)을 사용하여 관계를 암호화하십시오.

경제 잔액 모니터링 - 무단 구매와 관련하여 대출 기관 및 은행 카드 청구를 정기적으로 확인하십시오. 의심스러운 행동을 관찰하는 경우 즉시 일반 은행에 기록하십시오.

온라인 사기 방지

개인 안전 외에도 조직은 소비자와 비즈니스 정보를 보호하기 위해 사기 감소 전략을 적용해야 합니다. 여기에는 사기 탐지기 컴퓨터 소프트웨어 사용, 의심스러운 행동과 관련된 구매 감독, 직원에게 사이버 보안 모범 사례 교육이 포함됩니다. 전자 상거래 웹사이트의 경우 보호된 거래 게이트웨이와 SSL 암호화를 사용하면 안전한 구매가 보장됩니다. 또한 조직은 정보 침해를 방지하기 위해 정보 보호 법률과 규정을 준수해야 합니다.

마지막 생각

사이버 위험이 훨씬 더 우월해짐에 따라 온라인 보안과 사기 감소를 우선시하는 것이 모든 사람에게 중요합니다. 강력한 비밀번호를 실행하고, 2단계 인증을 허용하고, 피싱 사기에 대해 경계를 유지함으로써 사람들은 자신의 온라인 기본 보안을 쉽게 강화할 수 있습니다. 조직은 소비자 정보를 보호하고 사기를 방지하기 위한 실행 방법을 습득해야 합니다. 사이버 보안 스타일에 대해 계속 교육하고 안전한 온라인 행동을 실행하면 위험을 줄이고 더욱 안전한 전자 디지털 지식을 확보하는 데 도움이 될 수 있습니다.