온라인 보안 및 사기 방지: 전자 디지털 세계에서 위험을 감수하지 않는 방법

우리의 삶의 많은 요소가 온라인에서 변화함에 따라 온라인 보안 및 사기 감소를 확실히 하는 것이 그 어느 때보다 훨씬 더 중요해졌습니다. 사이버 범죄자들은 중요한 데이터를 빼내고, 경제적 사기를 저지르고, 취약점을 이용하기 위해 끊임없이 새로운 솔루션을 만들어냅니다. 소비자 뱅킹, 구매, 소셜 미디어 마케팅 또는 기업과 관련하여 온라인 비즈니스를 만들고 있든 컴퓨터 데이터와 ID를 메이저사이트 보호하려면 직접적인 방법이 필요합니다. 일반적인 위협을 이해하고 보안 권장 사항을 실행하기만 하면 온라인 사기의 희생자가 될 가능성을 크게 줄일 수 있습니다.

빈번한 사이버 위협

피싱 공격 - 이러한 사기에는 인공적인 이메일 메시지, 문자 메시지 또는 비밀번호 및 신용 카드 번호와 같은 민감한 정보를 제공하도록 사람들을 직접 유도하도록 만들어진 사이트가 포함됩니다.

스파이웨어와 애드웨어 및 랜섬웨어 - 악성 컴퓨터 소프트웨어는 감염된 백링크, 다운로드 또는 이메일 메시지를 통해 사용자 시스템에 설치될 수 있습니다. 랜섬웨어는 데이터 파일을 손상시키고 액세스에 대한 거래를 요구합니다.

ID 도난 - 사이버 범죄자는 중요한 데이터를 가져가 남성과 여성을 사칭하거나 대출 옵션을 신청하거나 무단 인수를 돕습니다.

정보 침해 - 온라인 범죄자는 조직과 사이트를 표적으로 삼아 소비자 데이터 소스에 액세스하여 사용자 이름, 비밀번호 및 경제 정보와 같은 매우 민감한 세부 정보를 공개합니다.

온라인 보안에 대한 권장 사항

특수하고 강력한 비밀번호 사용 - 여러 잔액에서 비밀번호를 재사용하지 마십시오. 대신 다양한 서신, 수량 및 특정 영웅을 사용하여 복잡한 비밀번호를 생성하십시오. 모든 비밀번호 관리자는 이를 견고하게 기록하는 데 도움이 됩니다.

2단계 인증(2FA) 허용 – 여러 온라인 회사에서 2FA를 제공하는데, 일반적으로 다음 증명 단계가 필요합니다. 예를 들어 휴대전화로 프로그램 코드를 전송하여 온라인 범죄자가 잔액에 액세스하는 것을 더욱 어렵게 만듭니다.

컴퓨터 소프트웨어와 가젯을 최신 상태로 유지하세요 – 시스템, 바이러스 백신 프로그램 및 프로그램에 대한 일반적인 개정 사항은 온라인 범죄자가 활용할 수 있는 보안 취약점을 해결합니다.

이메일 메시지와 백링크에 주의하세요 – 알려지지 않았거나 의심스러운 옵션에서 백링크를 선택하거나 부품을 다운로드하지 마세요. 사기꾼은 일반적으로 평판이 좋은 조직을 사칭하여 사람들에게 중요한 데이터를 공개하도록 직접 유도합니다.

웹 관계 보호 – 커뮤니티 Wi-Fi 사이트는 일반적으로 사이버 공격의 위험에 처해 있습니다. 컴퓨터 데이터를 암호화하기 위해 보장되지 않은 사이트를 탐색할 때는 전자 전용 커뮤니티(VPN)를 사용하세요.

경제적 구매에 주의하세요 - 정기적으로 대출 기관과 은행 카드 청구서를 확인하여 승인되지 않은 구매가 있는지 확인하세요. 대출 기관에 의심스러운 활동이 있으면 즉시 기록하세요.

온라인 구매에서 사기 방지

조직과 개인은 온라인에서 경제적 구매를 실행할 때마다 사기를 막기 위한 조치를 취해야 합니다. 전자 상거래 사이트는 보호된 거래 게이트웨이와 SSL 암호화를 사용하여 소비자 정보를 보호해야 합니다. 구매자는 신뢰할 수 있는 사이트에서만 쇼핑하고 링크 내에서 HTTPS와 같은 보안 특성을 검증하고 식별된 보안 공급업체의 봉인을 신뢰해야 합니다.

요약

인터넷은 편리함을 제공하지만 모든 것이 위험과 함께 판매됩니다. 사이버 위협을 알고 온라인 보안 및 사기 감소 권장 사항을 따르면 개인 및 경제적 정보를 보호하는 데 도움이 될 수 있습니다. 소비자이든 회사 소유자이든 강력한 암호, 2단계 인증 및 보호된 구매와 같은 사이버 보안 조치를 우선시하면 덜 위험한 온라인 지식을 개발하는 데 도움이 될 수 있습니다. 사이버 범죄자들을 멀리하기 위해 계속 교육하고 주의를 기울이십시오.