인터넷을 통한 건강한 생활: 보안 및 사기 방지의 필수적인 요령

오늘날의 인터넷 국가에서 인터넷 보안 및 안전과 더불어 사기 예상은 이 정상적인 활동의 정말 중요한 측면이 되고 있습니다. 사이버 위험을 향상시키고 해커가 사용하는 정교한 힌트를 통해 인터넷을 통한 개인 정보 보호는 그 어느 때보다 훨씬 더 가치가 있습니다. 토토사이트 인터넷, 은행 및 대출을 통해 조사하거나 단순히 쇼핑할 때 중요한 컴퓨터 데이터를 보존하는 방법을 이해하면 사기를 방지하고 건강을 유지할 수 있습니다.

일반적인 인터넷 위험

인터넷 위험은 여러 가지 다른 형태로 작용하며, 개인을 아는 것은 일반적으로 웹사이트에 대한 보호입니다. 가장 일반적인 단점은 다음과 같습니다.

피싱 이러한 사기: 사기꾼은 입증된 자산에서 직접 볼 수 있는 가짜 이메일이나 문자를 보내 개인을 속여 보안 암호 및 비자 또는 마스터카드 정보와 같은 기밀 정보를 노출시킵니다.

스파이웨어 및 랜섬웨어: 사악한 프로그램은 모든 기기를 공격하여 해커에게 개인 통계에 액세스할 수 있는 권한을 부여하거나 몸값을 지불하지 않는 한 모든 기록을 잠글 수 있습니다.

1. d. 범죄: 사이버 범죄자는 개인 정보를 유출하여 다른 사람을 사칭하고 사기를 치며, 여기에는 신용 점수 부채 또는 다른 사람의 목록에 대한 의료 기록 세금 명세서가 포함됩니다.

웹 보안을 보완하기 위한 제안

인터넷을 통해 신체를 보호하기 위해 할 수 있는 효과적인 방법은 다음과 같습니다.

강력한 보안 암호 및 2단계 인증 활용

훌륭한 암호는 첫 번째 독특한 방어선입니다. 메모, 정보 및 가치에 대한 혼란스러운 조합을 활용하세요. 일반적인 조건 또는 추측 가능한 정보를 피하세요.

가능하면 보안 및 안전에 대한 통합 계층에 2단계 인증(2FA)을 허용하세요. 결과적으로 비밀번호를 입력한 후 지역 번호를 전화로 보내는 것과 같은 후속 단계를 거쳐 모든 ID를 증명해야 합니다.

이메일 및 연결을 통해 주의하세요

이메일을 받은 후 의심스러운 연결이나 장치를 누르지 마세요. 특히 주제가 개인 정보를 요구하는 경우 답하기 전에 모든 발신자의 ID를 평가하세요. 이메일 피싱은 종종 긴급성에 대한 의미를 내포하여 환자를 짧은 행동으로 불안하게 만듭니다.

프로그램 및 기기를 새 것으로 유지하세요

오래된 프로그램은 대부분 해커의 일반적인 특정 대상입니다. 다음 보안 및 안전 비트를 받았는지 확인하려면 모든 운영 체제, 바이러스 백신 서비스 및 구직 신청서에 정기적으로 게시하세요.

모든 Wi-Fi 모바일 네트워크 보장

개인 재산 Wi-Fi 모바일 네트워크는 강력한 비밀번호를 사용하여 보호해야 합니다. 인터넷 은행 및 대출을 포함한 기밀 금융 거래에만 일반 Wi-Fi를 사용하지 말고, 모든 채권을 암호화하기 위해 훌륭한 인터넷 전문 모바일 전화 네트워크(VPN)를 선택하십시오.

부채 부채를 습관적으로 표시

담보 대출 기관 기록과 신용 파일을 자세히 살펴보십시오. 기이한 모험은 사기에 대한 원래 힌트라고 주장합니다. 그늘진 금융 거래를 기록한 후에는 자동으로 담보 대출 기관이나 비자 또는 마스터카드 통신사에 개인을 등록하십시오.

인터넷 사기로 인해 사상자가 된 경우 수행할 작업

지침을 선택하는 데 직면하여 거의 모든 사람이 인터넷 사기로 인해 사상자가 될 수 있습니다. 이런 일이 발생하면 매우 신속하게 행동하십시오.

변경된 부채를 냉동하기 위해 모든 은행에 연락하십시오.

모든 보안 암호를 자동으로 변경하십시오.

모든 사건을 집중된 법 집행 기관, 예를 들어 전국 운영 금융 위원회(FTC) 또는 모든 국가의 사이버 범죄 분리에 대해 설명하세요.

결과

인터넷 보안 및 안전과 사기 방지는 주의가 필요한 반복적인 과정입니다. 일반적인 위험에 익숙해지고 모범 사례를 고수하기만 해도 위험을 크게 줄일 수 있습니다. 기억하세요: 최신 정보를 파악하고 경계하는 것이 사이버 범죄로부터 자신을 보호하는 최고의 방벽입니다.