

# 온라인 보안 및 사기 예방: 전자 시대에서 자신을 보호하세요

웹은 연결, 저장 및 회사 운영 방식에 혁명을 일으켰지만 사이버 보안 위험과 온라인 사기도 증가시켰습니다. 온라인 범죄자와 사기꾼이 끊임없이 전략을 변경함에 따라 개인 및 금융 정보를 보호하기 **액티브검증** 위해서는 온라인 보안 및 사기 방지에 대한 지식이 중요합니다. 인터넷을 검색하는 사람이든 고객 정보를 처리하는 회사이든 적극적인 조치를 취하면 사이버 범죄의 표적이 될 위험을 상당히 줄일 수 있습니다.

## 온라인 위험에 대한 지식

사이버 범죄자는 피싱 에피소드, 애드웨어 및 스파이웨어 감염, 신원 도용 및 금융 사기와 같은 취약점을 이용하기 위해 다양한 전략을 사용합니다. 피싱 사기에는 사기성 이메일, 커뮤니케이션 또는 웹사이트가 포함되어 고객을 속여 보안 비밀번호 또는 금융 정보와 같은 민감한 정보를 노출시킵니다. 해로운 소프트웨어 프로그램에 대한 간략한 설명은 해로운 다운로드 또는 의심스러운 하이퍼링크를 통해 제품을 침범하여 온라인 범죄자가 정보를 훔치거나 신체를 제어할 수 있도록 허용합니다. 사기꾼이 개인 정보에 접근하여 신용 회사 계정을 개설하거나 무단 구매를 하는 등 사기를 저지르기 위해 이를 사용할 때 신원 도용이 발생합니다.

## 온라인 보호를 위한 중요한 전략

**강력한 보안 비밀번호 사용** - 강력한 비밀번호는 최소 **12**자리 길이어야 하며 대문자, 소문자, 숫자 및 고유한 아이콘을 혼합해야 합니다. 생일이나 일반적인 문구와 같이 쉽게 의심되는 보안 비밀번호를 사용하지 마십시오. 복잡한 보안 비밀번호를 견고하게 쇼핑하려면 비밀번호 관리자를 사용하는 것을 고려하십시오.

**2단계 인증(2FA) 허용** - 보호와 관련된 추가 코팅을 포함하여, 전화기로 전송되는 증거 신호와 같이, 온라인 범죄자가 귀하의 회사 계정에 침투하는 것을 상당히 어렵게 만듭니다. 비록 이들이 귀하의 비밀번호를 얻었더라도요.

**소프트웨어 및 제품을 최신 상태로 유지** - 자주 업그레이드하는 시스템, **Forefox** 브라우저 및 보호 소프트웨어 프로그램은 사이버 범죄자가 이용할 수 있는 취약점을 탐지하는 데 도움이 됩니다. 자동화된 개선 사항을 통해 최신 보안도 제공됩니다.

**이메일 및 하이퍼링크에 주의하세요** - 피싱 사기는 종종 은행, 소셜 네트워킹 시스템 또는 소매업체를 통한 진짜 마케팅 커뮤니케이션인 것처럼 위조된 커뮤니케이션을 숨깁니다. 의심스러운 하이퍼링크를 클릭하거나 익숙하지 않은 리소스를 통해 장치를 다운로드하지 마세요.

**웹 링크 보호** - 민감한 거래의 경우 공개 **Wi-Fi**를 사용하지 마세요. 온라인 범죄자가 보호되지 않은 시스템에서 정보를 가로챌 수 있기 때문입니다. 공공 장소에서 웹에 접속할 수 있는 경우, **VPN**(디지털 개인 시스템)을 사용하여 자신의 연결을 암호화하세요.

금융 회사 계좌 추적 - 승인되지 않은 거래에 대한 금융 기관 및 신용카드 청구를 자주 확인하세요. 의심스러운 활동을 발견하면 즉시 대출 기관에 신고하세요.

## 온라인 사기 중단

개인 보호를 넘어 회사는 고객과 조직 정보를 보호하기 위해 사기 방지 방법을 실행해야 합니다. 여기에는 사기 감지 소프트웨어 프로그램 사용, 의심스러운 활동과 관련된 거래 확인, 사이버 보안 권장 사항에 대한 직원 연구 등이 포함됩니다. 전자 상거래 웹사이트의 경우 안전한 지불 게이트웨이와 **SSL** 암호화를 사용하면 안전한 거래가 보장됩니다. 또한 회사는 정보 침해를 방지하기 위해 정보 보안 규정을 준수해야 합니다.

## 요약

사이버 위험이 더욱 심화됨에 따라 인터넷 보호 및 사기 방지를 우선시하는 것이 모든 사람에게 중요합니다. 강력한 보안 암호를 적용하고, 2단계 인증을 허용하고, 피싱 사기에 대해 조심함으로써 사람들은 인터넷 보안을 개선할 수 있습니다. 회사는 또한 고객 정보 저장 사기를 보호하기 위한 적극적인 조치를 고려해야 합니다. 사이버 보안 개발에 대한 지식을 유지하고 안전한 인터넷 일상을 훈련하면 위험을 줄이고 훨씬 더 안전한 전자적 경험을 보장하는 데 도움이 될 수 있습니다.