

안전한 온라인 बैं킹을 위한 8가지 팁

1 자신의 계좌를 정기적으로 모니터링 할 것.

게시된 모든 거래가 자신이 승인한 거래인지 확인합니다. 사기 또는 미심쩍은 활동으로 여겨지는 경우 즉시 은행에 신고합니다.

2 이상한 이메일을 조심할 것!

자신의 은행(또는 다른 회사)에서 발송했다고 주장하는 이메일에 귀하의 계좌 정보나 비밀번호를 요청할 경우 이에 응답하지 말아야 합니다. 은행에서는 귀하의 계좌 정보를 묻기 위해 이메일을 통해 귀하에게 연락하지 않습니다.

3 이메일의 링크를 클릭하지 말 것.

일반적으로 은행 웹사이트에 수동으로 로그인하여 보안 사이트에 들어가는 것이 훨씬 더 안전합니다

4 수시로 은행 비밀번호를 변경할 것.

여러 사이트에서 같은 비밀번호를 사용하지 말고 대문자와 소문자, 숫자, 특수 문자가 혼합된 강력한 비밀번호를 선택해야 합니다. 자신의 이름, 이니셜, 생년월일이 포함된 단어나 문구를 사용하지 말아야 합니다.

5 이중 인증을 활성화합니다.

많은 금융 기관에서는 예금주를 위한 보안 단계를 추가했습니다. 이중 인증을 사용하려면 계정에 접속하기 전에 추가 확인 자격 인증을 입력해야 합니다.

6 자동 로그인을 비활성화합니다.

자신의 웹 브라우저에서 자신의 온라인 बैं킹 웹사이트에 대한 개인 사용자 이름과 비밀번호 정보를 저장하도록 노출하여서는 안 됩니다.

7 가능한 한 은행의 공식 모바일 앱만 사용할 것.

그리고 애플 스토어나 구글 플레이 스토어 등 평판이 좋은 소스에서 앱을 다운로드합니다.

8 어떤 것이 합법적인지 확실하지 않은가요?

은행의 기술력에 대해 궁금한 점이 있으신가요? 전화주시면 기꺼이 도와드릴 것입니다!

다음 협력업체를 통해 귀하에게 제공되었습니다:



사이버 보안을 더욱 강화하기 위한 8가지 팁

1 이메일 사기

사실이라고 하기에는 너무 괜찮아 보인다면 사기일 가능성이 높습니다. 외국에서 온 복권 관계 직원이나 왕자들이 이메일로 연락할 것이라고 한다면 믿어서는 안됩니다!

2 사기성 결제

위조 수표, 자기앞 수표, 우편환 또는 돈의 일부를 현금해 달라고 요청하는 전자 자금 이체를 조심하십시오.

3 미심쩍은 제안

“빠른 행동”을 요구하는 미심쩍은 제안에 주의하셔야 합니다.

4 최신 상태를 유지하기

Windows, Apple iOS, 휴대폰 IOS(Apple, Android 등) 등 운영 체제에 대한 최신 보안 업데이트로 장치가 최신 상태인지 반드시 확인하셔야 합니다.

5 경고 및 오류

인증서 경고나 오류가 있는 웹사이트를 신뢰하지 말아야 합니다.

6 이메일 첨부파일을 주의할 것

출처를 알 수 없는 이메일 첨부 파일이나 무료 소프트웨어를 클릭하는 것은 결코 좋은 생각이 아닙니다. 결국 시스템이 온라인 사기 및 도난에 노출될 수 있습니다.

7 온라인 공유

온라인에서 얼마나 공유가 되고 있는지 살펴볼 것. 귀하가 소셜 네트워킹 사이트에 자신에 대해 더 많이 게시할수록 누군가가 해당 정보를 사용하여 귀하의 계정에 접속하고 귀하의 신분을 도용하는 등의 작업이 더 쉬워질 수 있습니다. 개인 정보 보호 설정을 최대화하여 개인 정보를 보호해야 합니다.

8 금융 사기

재난 관련 금융 사기에 주의할 것. 사기꾼은 재난 사건이 발생한 후 합법적인 자선 단체 소속이라고 주장하면서 사람들을 이용합니다. 실제로는 돈이나 귀중한 개인 정보를 훔치려고 시도할 것입니다.

온라인 안전에 관한 추가 자료:

텍사스 은행부서 - www.dob.texas.gov

텍사스 은행가 협회 - www.texasbankers.com/

BankingSafely

더 나은 사업 관리국 - www.bbb.org/council/

for-businesses/cybersecurity/