거래 및 계정 보안

계정 보안은 당사에 중요한 사안이며, 당사는 귀하의 Remitly 계정 관련 정보를 보호하기 위해 여러 가지 조치를 취하고 있습니다. 귀하도 본인의 계정과 개인 정보 보호를 위해 하실 수 있는 것이 있습니다.

계정 인증 절차

높은 수준의 보안, 신뢰 및 보호를 유지하기 위해 귀하의 Remitly 계정에는 인증 절차가 적용되고 있습니다.

Remitly에 새로 가입해 Remitly 웹사이트에서 새로 Remitly 계정을 만드신 경우 반드시 일정한 개인 정보를 제공해 이메일 인증 절차를 완료해 주셔야 합니다.

일단 계정이 사용 가능해지면 당사에서 의심스러운 계정 활동을 파악할 수 있게 도와주는 다양한 수동 및 자동 리스크 관리 절차를 실시하게 됩니다. 이러한 절차의 목표는 특이하거나 귀하의 과거 사용 이력에 부합되지 않는 것으로 보이는 특징을 식별하는 것입니다. 당사는 이러한 절차의 일환으로 개인 정보 및 금융 정보 인증을 위해 업계 선두 서비스 제공업체들과 계약을 맺고 있습니다. 이러한 서비스 업체들은 절대 귀하에게 직접 연락하지 않으며, 귀하의 정보는 귀하가 의도한 거래가 성공적으로 완료되도록 하는 목적 외에는 사용하지 않습니다.

암호 보안

당사는 이용자가 본인 계정이 로그인할 때 이용자 계정 보호를 위해 일정한 조치를 취합니다. 첫째, 본인 Remitly 계정에 로그인할 때 보안 서버 연결을 사용해 로그인하게 됩니다(https://). 당사는 보안 서버 보호 부문 업계 표준으로 256 비트 암호화가 적용되는 SSL(Secure Socket Layer)을 사용합니다.

귀하의 계정은 본인이 만드는 고유한 암호로도 보호됩니다. 흔히 쓰는 단어나 구문을 암호로 사용해서는 안 됩니다. 대신, 암호는 대문자와 소문자, 숫자를 모두 포함해 최소 8자리로 만들어야 합니다. 암호는 본인만 알고 있어야 합니다. 암호를 공유하는 경우 Remitly 계정의 보안성이 저하됩니다.

인터넷 사기에 주의하십시오

- 절대 복권이나 경품 당첨금을 받기 위해, 또는 큰 금액의 돈을 준다는 약속을 듣고 송금하지 마십시오.
- 절대 신용카드나 대출을 “보장”해 준다는 이유로 송금하지 마십시오.
- 절대 인터넷이나 전화로 받고 정직한 것인지 여부가 확실치 않은 제안에 응답하지 마십시오.
- 절대 모르는 사람이나 신분을 인증할 수 없는 사람에게 송금하지 마십시오.

의심이 되는 경우 돈을 받겠다는 사람에게 요청한 돈의 목적과 안전성에 대해 자세한 정보를 요청하십시오. 거래에 대한 확신이 들 때 까지는 절대 송금을 하지 마십시오.

피싱 또는 스푸핑 이메일 식별 방법

얼핏 보기에 Remitly가 보낸 것처럼 보이는 이메일이지만 실제로는 진짜가 아닌 이메일을 받는 경우가 있으실 겁니다. 그런 이메일은 Remitly 웹사이트와 비슷해 보이는 웹사이트로 안내할 수 있습니다. 그런 웹사이트로 가면 이메일 주소와 암호 등, 계정 정보를 입력해 달라는 요청을 받으실 수도 있습니다.

이런 가짜 웹사이트는 사기를 저지르기 위해 귀하의 민감한 계정 및 결제 정보를 훔칠 수 있습니다. 이런 가짜 이메일에는 암호나 민감한 데이터를 감지할 수 있는 바이러스나 맬웨어가 담겨 있을 수 있습니다. 따라서 안티바이러스(백신) 프로그램을 설치하고 항상 업데이트 상태를 유지하는 것이 좋습니다.

다음은 사기성 이메일에 대비한 방어책의 일환으로 항상 기억하고 계셔야 할 몇 가지 중요 사항입니다:

- 이용자의 전체 SSN(사회 보장 번호) 또는 생년월일
- 이용자의 신용카드 번호, PIN 또는 신용카드 보안 코드(위 정보의 “업데이트된 정보” 포함)

의심스럽거나 알지 못하는 발송자가 보낸 이메일 첨부 파일은 열지 않는 것이 좋습니다. 이메일 첨부 파일에는 열었을 때 사용자의 컴퓨터를 감염시키는 바이러스가 담겨 있을 수 있습니다. Remitly가 보낸 것으로 위장한 의심스러운 이메일을 받았는데 파일이 첨부되어 있는 경우 첨

부 파일을 열지 말고 바로 메일을 삭제하시는 것이 좋습니다.

문법적으로 부실하거나 오탈자 실수가 있는지 눈여겨봅니다. 피싱 이메일 중에는 다른 언어를 번역한 것이거나 작성 후 검토 없이 발송되면서 문법이나 오탈자 실수가 포함되어 있는 경우가 있습니다.

Remitly가 보낸 이메일이 맞나? 피싱 범죄자들이 Remitly가 보낸 것처럼 보이게 하려고 이메일을 위조할 수 있지만 반송 주소를 보면 정말 Remitly에서 보낸 것인지 여부를 확인할 수 있는 경우가 많습니다. 이메일의 “보낸 사람” 란의 주소가 “remitly-security@hotmail.com”이나 “remitly-fraud@msn.com” 등인 경우, 또는 다른 인터넷 서비스 제공업체 이름이 포함되어 있는 경우 가짜 이메일인 것을 확실히 알 수 있습니다.

진짜 Remitly 웹사이트는 항상 다음 도메인에서 호스팅합니다: https://www.remitly.com/

스푸핑 이메일에 포함되어 있는 링크가 실제 Remitly 주소처럼 보이는 경우도 있습니다. 그 링크 위로 마우스를 가져가 보면 실제 이동 주소가 어디인지 확인할 수 있습니다. 사용하고 계신 브라우저 창의 하단에 있는 상태 표시줄이나 팝업창 안에 그 링크의 실제 이동 웹사이트가 나타납니다.

당사는 위에 안내해 드린 도메인이 아닌 다른 도메인에서 호스팅하는 웹 주소를 절대 사용하지 않습니다. 예를 들어, 약간 변형한 도메인, "http://security-payments-remitly.com/. . .” 또는 IP 주소(숫자열) 뒤에 디렉터리가 붙은 형태, “http://123.456.789.123/remitly.com/. . .”는 유효한 Remitly 웹사이트가 아닙니다.

또한, 스푸핑한 이메일을 열고 본문 중 아무 곳이나 클릭해도 사기성 웹사이트로 이동하도록 설정해 둔 경우도 있습니다. Remitly는 절대 그런 형태의 이메일을 보내지 않습니다. 실수로 그런 이메일을 클릭해 스푸핑 웹사이트로 이동하게 되신 경우 아무런 정보도 입력하지 않은 채로 브라우저 창을 닫아버리시면 됩니다.

의심이 드는 경우 이메일에 들어 있는 링크를 클릭하지 마십시오. https://www.remitly.com/으로 바로 가서 우측 상단에 있는 메뉴 중 **Your Account** (내 계정)를 클릭해 최근 구입 내역이나 내 계정 정보를 확인하시면 됩니다. 본인 계정에 액세스하실 수 없거나 조금이라도 의심스러운 부분이 발견되는 경우 즉시 당사에 알려 주십시오.

스푸핑 이메일이나 의심스러운 이메일을 클릭해 이동한 다음 본인의 Remitly 계정 정보를 입력하신 경우 **즉시** 암호를 변경하셔야 합니다. https://www.remitly.com/으로 직접 이동

해 **Account Settings**(계정 설정)을 클릭하시면 됩니다. 다음 페이지에서 **Change your personal information, e-mail address, or password**(개인 정보, 이메일 또는 암호 변경)를 클릭합니다.

위조된 이메일 메시지에서 링크 연결된 사이트로 신용카드 번호를 제출하신 경우 본인 정보 보호를 위한 조치를 취하시는 것이 좋습니다. 예를 들어 해당 신용카드 회사에 연락해 상황을 알리도록 하십시오. 마지막으로, 누구든 귀하 계정에 부정한 방법으로 액세스하지 못하도록 본인 Remitly 계정에서 해당 신용카드를 삭제해야 합니다.

위조임이 확실한 이메일을 받았거나, 본인이 피싱 공격을 당했고 본인 Remitly 계정 보안이 우려되는 경우 [피싱 또는 스푸핑 이메일](/home/contact/)을 신고해 즉시 당사에 알려 주시기 바랍니다.