# Transaction and Account Security

Account security is important to us and we've taken several steps to protect your Remitly account-related information. You too can do certain things that will help protect your account and personal information.

## Account Verification Processes

Your Remitly account is subject to verification procedures to maintain high levels of security, trust, and protection.

If you are a new Remitly customer and you create a new Remitly account using the Remitly website, you must provide certain personal information and complete the e-mail verification process.

Once your account is up and running we deploy a variety of manual and automated risk management procedures that allow us to highlight suspicious account activity. The goal is to identify any characteristics that seem unusual or inconsistent with your past usage. As part of this process we contract with industry leading service providers to verify personal and financial information. These services will never contact you directly or use your information for anything but the successful completion of your intended transaction.

## Password Security

When you log in to your account we do certain things to protect your account. First, whenever you log in to your Remitly account, you log in using a secure server connection (https://). We use Secure Socket Layer (SSL) with 256-bit encryption, the industry standard in secure server protection.

Your account is also protected by a unique password that you create. You should not use common words or phrases as your password. Instead, your password should be at least eight characters including both numbers and letters using

upper and lower cases. You should keep this password confidential. Sharing your password will lessen the security of your Remitly account.

## Be Wary of Internet Scams

- DO NOT make a payment to claim lottery or prize winnings, or on a promise of receiving a large amount of money.
- DO NOT make a payment because you are "guaranteed" a credit card or loan.
- DO NOT respond to an Internet or phone offer that you aren't sure is honest.
- DO NOT make a payment to someone you don't know or whose identity you can't verify.

When in doubt, ask the intended recipient for more information about the purpose and safety of the requested payment. Do not send the payment until you are comfortable with the transaction.

## Identifying Phishing or Spoofed E-mails

You may at some time receive an e-mail that looks like it came from Remitly, but is in fact not genuine. Such an e-mail may direct you to a website that looks similar to the Remitly website. You might even be asked to provide account information such as your e-mail address and password.

These false websites can steal your sensitive account and payment information in order to commit fraud. These false e-mails may contain potential viruses or malware that can detect passwords or sensitive data. We therefore recommend that you install an anti-virus program and keep it updated at all times.

Here are some key points to keep in mind as part of a defense against fraudulent e-mails:

- Your full social security number or date of birth
- Your credit card number, PIN, or credit card security code

(including "updates" to any of the above)

We recommend that you not open any e-mail attachments from suspicious or unknown sources. E-mail attachments can contain viruses that infect your computer when the attachment is opened. If you receive a suspicious e-mail purportedly sent from Remitly that contains an attachment we recommend that you delete the e-mail, without opening the attachment.

Look for poor grammar or typographical errors. Some phishing e-mails are translated from other languages or are sent without being proofread, and as a result, contain bad grammar or typographical errors.

Is the e-mail from Remitly? While phishers can send a forged e-mail to make it look like it came from Remitly, you can sometimes determine whether it's authentic by checking the return address. If the "from" line of the e-mail looks like "remitly-security@hotmail.com" or "remitly-fraud@msn.com", or contains the name of another Internet service provider, you can be sure it’s not genuine.

Genuine Remitly websites are always hosted on the following domain: [https://www.remitly.com/](https://www.remitly.com/)

Sometimes the link included in spoofed e-mails looks like a genuine Remitly address. You can check where it actually points to by hovering your mouse over the link--the actual website where it points to will be shown in the status bar at the bottom of your browser window or as a pop-up.

We never use a web address hosted on a domain other than the ones listed above. For instance, variant domains such as "https://security-payments-remitly.com/. . ." or an IP address (string of numbers) followed by directories such as "https://123.456.789.123/remitly.com/. . ." are not valid Remitly websites.

Also, sometimes the spoofed e-mail is set up such that if you click anywhere on the text you are taken to the fraudulent website. Remitly will never

send an e-mail that does this. If you accidentally click on such an e-mail and go to a spoofed website, do not enter any information; instead, just close that browser window.

When in doubt, do not click the link included in an e-mail. Go directly to [https://www.remitly.com/](https://www.remitly.com/) and click **Your Account** in the top right menu to view recent purchases, or review your account information. If you cannot access your account, or if you see anything suspicious, let us know right away.

If you did click through from a spoofed or suspicious e-mail and you entered your Remitly account information, you should **immediately** update your password. You can do this by going directly to https://www.remitly.com/ and clicking **Account Settings**. On the next page, click the **Change your personal information, e-mail address, or password**.

If you submitted your credit card number to the site linked to from the forged e-mail message, we advise that you take steps to protect your information. You might want to contact your credit card company, for example, to notify them of this matter. Finally, you should delete that credit card from your Remitly account to prevent anyone from improperly regaining access to your account.

If you have received an e-mail you know is a forgery, or if you think you have been a victim of a phishing attack and you are concerned about your Remitly account, please let us know right away by reporting a [phishing or spoofed e-mail](/home/contact/).