Seguridad ng Transaksyon at Account

Mahalaga sa amin ang seguridad ng account at gumawa kami ng ilang hakbang para protektahan ang impormasyong nauugnay sa Remitly account mo. Maaari ka ring gumawa ng ilang bagay na makakatulong na maprotektahan ang iyong account at personal na impormasyon.

Mga Proseso ng Pag-verify sa Account

Ang iyong Remitly account ay sumasailalim sa mga proseso ng verification para mapanatili ang matataas na antas ng seguridad, tiwala, at proteksyon.

Kung isa kang bagong customer ng Remitly at gumawa ka ng bagong Remitly account gamit ang Remitly website, dapat kang magbigay ng ilang personal na impormasyon at dapat mong kumpletuhin ang proseso ng verification sa e-mail.

Kapag gumagana na ang iyong account, gumagamit kami ng ilang mano-mano at awtomatikong paraan ng pamamahala sa panganib na nagbibigay-daan sa aming mag-highlight ng kahina-hinalang aktibidad sa account. Ang layunin ay matukoy ang anumang mga katangiang mukhang hindi pangkaraniwan o hindi katulad ng nakaraan mong paggamit. Bilang bahagi ng prosesong ito, nakikipagkontrata kami sa mga service provider na nangunguna sa industriya para ma-verify ang personal at pinansyal na impormasyon. Hindi ka kailanman direktang iko-contact ng mga serbisyong ito at hindi nito kailanman gagamitin ang iyong impormasyon para sa anumang bagay maliban sa matagumpay na pagkumpleto ng nilalayon mong transaksyon.

Seguridad ng Password

Kapag nag-log in ka sa iyong account, gumagawa kami ng ilang bagay para maprotektahan ang iyong account. Una, sa tuwing naglo-log in ka sa iyong Remitly account, naglo-log in ka gamit ang isang secure na koneksyon sa server (https://). Gumagamit kami ng Secure Socket Layer (SSL) na may 256-bit encryption, ang pamantayan sa industriya para sa proteksyon ng secure na server.

Protektado din ang iyong account ng isang natatanging password na gagawin mo. Hindi ka dapat gumamit ng mga karaniwang salita o parirala bilang iyong password. Sa halip, ang iyong password ay dapat na may kahit walong character kasama ang mga numero at malalaki at maliliit na titik. Dapat mong panatilihing kumpidensyal ang password na ito. Ang pag-share sa iyong password ay makakabawas sa seguridad ng iyong Remitly account.

Mag-ingat sa mga Internet Scam

- HUWAG magbayad para ma-claim ang mga panalo sa loto o premyo, o dahil sa pangakong makakatanggap ng malaking halaga ng pera.
- HUWAG magbayad dahil binigyan ka ng "garantiyang" magkakaroon ka ng credit card o loan.
- HUWAG sumagot sa isang alok sa Internet o telepono kung saan hindi ka sigurado kung totoo ito.
- HUWAG magbayad sa isang taong hindi mo kilala o na may pagkakakilanlang hindi mo ma-verify.

Kung nagdududa ka, humiling sa nilalayong recipient ng higit pang impormasyon tungkol sa layunin at kaligtasan ng hiniling na pagbabayad. Huwag ipadala ang bayad hanggang sa maging kumportable ka sa transaksyon.

Pagtukoy sa Phishing o Spoofed E-mails

Minsan, posible kang makatanggap ng e-mail na mukhang nanggaling sa Remitly, pero hindi ito totoo. Ang naturang e-mail ay maaaring magdirekta sa iyo sa isang website na kamukha ng Remitly website. Posible pang hilingin sa iyong magbigay ng impormasyon ng account gaya ng iyong e-mail address at password.

Ang mga pekeng website na ito ay puwedeng magnakaw ng iyong sensitibong impormasyon sa account at pagbabayad upang magsagawa ng panloloko. Ang mga pekeng e-mail na ito ay maaaring maglaman ng mga potensyal na virus o malware na kayang mag-detect ng mga password o sensitibong data. Samakatuwid, inirerekomenda naming mag-install ka ng anti-virus program at panatilihin mo itong updated sa lahat ng pagkakataon.

Narito ang ilang mahahalagang puntong dapat tandaan bilang bahagi ng depensa laban sa mga mapanlokong e-mail:

- Ang iyong buong social security number o petsa ng kapanganakan
- Ang iyong credit card number, PIN, o credit card security code (kasama ang "mga update" sa alinman sa itaas)

Inirerekomenda naming huwag kang magbukas ng anumang mga e-mail attachment mula sa mga kahina-hinala o hindi kilalang pinagmulan. Ang mga e-mail attachment ay maaaring maglaman ng mga virus na nakaka-infect sa iyong computer kapag binuksan ang attachment. Kung makakatanggap ka ng kahina-hinalang e-mail na ipinadala raw ng Remitly na naglalaman ng attachment, inirerekomenda naming i-delete mo ang e-mail, nang hindi binubukdan ang attachment.

Maghanap ng maling grammar o mga typographical error. Ang ilang phishing e-

mail ay tina-translate mula sa ibang mga wika o sine-send nang hindi pinu-proofread, at bilang resulta ay naglalaman ng maling grammar o mga typographical error.

Mula ba sa Remitly ang e-mail? Bagama't ang mga phisher ay puwedeng mag-send ng mga pekeng e-mail para magmukha itong nanggaling sa Remitly, minsan ay matutukoy mo kung totoo ito sa pamamagitan ng pagtingin sa return address. Kung ang linyang "from" ng e-mail ay katulad ng "remitly-security@hotmail.com" o "remitly-fraud@msn.com", o naglalaman ng pangalan ng ibang Internet service provider, makatitiyak kang hindi ito tunay.

Ang mga tunay na Remitly website ay palaging naka-host sa sumusunod na domain: https://www.remitly.com/

Minsan, ang link na kasama sa mga spoofed na e-mail ay kamukha ng isang tunay na Remitly address. Puwede mong tingnan kung saan talaga ito nagpo-point sa pamamagitan ng pag-hover ng iyong mouse sa link--ang aktwal na website kung saan ito nagpo-point ay ipapakita sa status bar sa ibaba ng iyong browser window o bilang isang pop-up.

Hindi kami kailanman gumagamit ng web address na naka-host sa isang domain maliban sa mga nakalista sa itaas. Halimbawa ang mga variant na domain gaya ng "https://security-payments-remitly.com/. . ." o isang IP address (string ng mga numero) na sinusundan ng mga directory tulad ng "https://123.456.789.123/remitly.com/. . ." ay hindi mga valid na Remitly website.

Gayundin, minsan ay naka-set up ang spoofed na e-mail nang sa gayon ay kapag nag-click ka kahit saan sa text ay dadalhin ka sa mapanlokong website. Hindi kailanman magpapadala ang Remitly ng e-mail na gumagawa nito. Kung aksidente kang magki-click sa naturang e-mail at pumunta ka sa isang spoofed na website, huwag maglagay ng anumang impormasyon; sa halip, isara lang ang browser window na iyon.

Kung nagdududa ka, huwag i-click ang link na kasama sa isang e-mail. Pumunta nang direkta sa https://www.remitly.com/ at i-click ang **Iyong Account** sa kanang menu sa itaas para tingnan ang mga kamakailang pagbili, o i-review ang impormasyon ng iyong account. Kung hindi mo ma-access ang iyong account, o kung nakakakita ka ng kahit anong kahina-hinala, ipaalam mo ito sa amin kaagad.

Kung nag-click ka sa isang spoofed o kahina-hinalang e-mail at inilagay mo ang impormasyon ng iyong Remitly account, dapat mong **agad** na i-update ang iyong password. Puwede mo itong gawin sa pamamagitan ng pagpunta nang direkta sa https://www.remitly.com/ at pag-click sa **Mga Setting ng Account**. Sa susunod na page, i-click ang **Palitan ang iyong personal na impormasyon, e-mail address, o password**.

Kung isinumite mo ang iyong credit card number sa site na naka-link mula sa pekeng e-mail message, pinapayuhan ka naming gumawa ng mga hakbang para protektahan ang iyong impormasyon. Maaari mo ring i-contact ang iyong credit card company, halimbawa, para i-notify sila tungkol sa isyung ito. Panghuli, dapat mong i-delete ang credit card na iyon sa iyong Remitly account para mahadlangan ang sinuman na magkaroon ulit ng access sa iyong account sa di-wastong paraan.

Kung nakatanggap ka ng e-mail na alam mong peke, o kung naging biktima ka ng isang phishing attack at nag-aalala ka tungkol sa iyong Remitly account, ipaalam ito kaagad sa amin sa pamamagitan ng pag-uulat ng [phishing o spoofed na e-mail](/home/contact/).