Varainsiirtotapahtumien ja tilin turvallisuus

Tilien turvallisuus on Remitlylle tärkeää, ja Remitly on ryhtynyt toimenpiteisiin omaan Remitly-tiliisi liittyvien tietojen suojaamiseksi. Voit myös itse auttaa oman tilisi ja henkilötietojesi suojaamisessa.

Tilin varmennusprosessit

Remitly-tiliisi kohdistetaan varmennustoimenpiteitä. Tällä ylläpidetään hyvää turvallisuutta, luottamusta ja suojaa.

Jos olet uusi Remitly-asiakas ja luot uuden Remitly-tilin Remitly-verkkosivustoa käyttämällä, on sinun annettava tiettyjä henkilötietoja ja täydennettävä sähköpostitse tapahtuva varmennusprosessi.

Kun tili on avattu ja käytettävissä, siihen kohdistetaan manuaalisia ja automatisoituja riskienhallintatoimenpiteitä, joilla epäilyttävä tilin käyttö voidaan huomata. Tavoitteena on havaita merkkejä, jotka ovat epätavallisia aiempaan käyttöösi verrattuna tai poikkeavat siitä. Tämän prosessin osana Remitly antaa alan johtaville palveluntarjoajille toimeksi henkilö- ja taloudellisten tietojen varmentamisen. Nämä palveluntarjoajat eivät ota sinuun koskaan suoraan yhteyttä eivätkä käytä tietojasi mihinkään muuhun kuin haluamasi varainsiirtotapahtuman onnistuneeseen täydentämiseen.

Salasanojen turvallisuus

Kirjautuessasi sisään omalle tilillesi sen suojaamiseksi tehdään tiettyjä toimenpiteitä. Ensinnäkin: aina, kun kirjaudut sisään omalle Remitly-tilillesi, se tapahtuu suojattua palvelinyhteyttä (https://) käyttämällä. Remitly käyttää SSL-salausprotokollaa (Secure Socket Layer) 256-bittisellä salauksella. Tämä on alan standardi turvalliselle palvelinten suojaamiselle.

Tiliäsi suojaa myös itse luomasi ainutkertainen salasana. Salasanana ei tule käyttää tavallisia sanoja tai lauseita. Salasanan tulisi sen sijaan koostua vähintään kahdeksasta merkistä sisältäen sekä numeroita että kirjaimia ja käyttäen sekä isoja että pieniä kirjaimia. Tämä salasana tulee pitää luottamuksellisena. Oman salasanan kertominen muille heikentää Remitly-tilisi turvallisuutta.

Varo internethuijauksia

- ÄLÄ suorita maksuja arvonta- tai kilpailuvoittojen lunastamiseksi tai koska sinulle on luvattu suuri määrä rahaa.
- ÄLÄ suorita maksua sillä perusteella, että sinulle on "taattu" jokin luottokortti

tai laina.

- ÄLÄ reagoi internet- tai puhelintarjoukseen, jos et ole varma, että se on aito.
- ÄLÄ suorita maksuja henkilöille, joita et tunne tai joiden henkilöllisyyttä et voi varmistaa.

Jos jokin asia epäilyttää, kysy aiotulta vastaanottajalta lisätietoja pyydetyn maksun tarkoituksesta ja turvallisuudesta. Älä suorita maksua ennen kuin kaikki varainsiirtoon liittyvä tuntuu olevan kunnossa.

Verkkourkinta- tai huijaussähköpostiviestien tunnistaminen

Saatat silloin tällöin saada sähköpostiviestin, joka näyttää tulevan Remitlyltä, mutta ei itse asiassa ole aito. Tällainen sähköpostiviesti saattaa ohjata sinut Remitlyn verkkosivustoa muistuttavalle verkkosivustolle. Sinua saatetaan jopa pyytää antamaan tilitietojasi, kuten sähköpostiosoitteesi ja salasanasi.

Nämä huijausverkkosivustot pystyvät varastamaan arkaluontoisia tili- ja maksutietoja petosten tekemistä varten. Näissä huijaussähköpostiviesteissä saattaa olla mahdollisia viruksia tai haittaohjelmia, jotka pystyvät selvittämään salasanoja tai arkaluontoisia tietoja. Remitly suositteleekin virustorjuntaohjelman asentamista ja sen pitämistä aina päivitettynä.

Tässä on muutamia keskeisiä seikkoja, jotka kannattaa pitää mielessä huijaussähköpostiviesteiltä puolustautumiseksi:

1. Tieto siitä, mitä Remitly ei kysy tai pyydä sähköpostitse

- täydellinen sosiaaliturvatunnus tai syntymäaika
- luottokortin numero, PIN tai luottokortin turvakoodi (mukaan lukien yllä olevien "päivitykset").

2. Varo epäilyttävien sähköpostiviestien liitteitä

Remitly suosittelee olemaan avaamatta epäilyttävistä tai tuntemattomista lähteistä peräisin olevia sähköpostiliitteitä. Sähköpostiliitteissä saattaa olla viruksia, jotka saastuttavat tietokoneen, kun liite avataan. Jos saat epäilyttävän sähköpostiviestin, joka on muka Remitlyltä ja joka sisältää liitteen, kannattaa kyseinen sähköpostiviesti poistaa liitettä avaamatta.

3. Katso, onko viestissä kielioppi- tai kirjoitusvirheitä

Katso, onko viestin tekstin kielioppi huonoa tai onko tekstissä kirjoitusvirheitä. Jotkut verkkourkintaviestit on käännetty muista kielistä tai ne on lähetetty ilman oikolukua, ja tämän tuloksena niissä on kielioppi- tai kirjoitusvirheitä.

4. Tarkista palautusosoite

Onko sähköpostiviesti Remitlyltä? Vaikka verkkourkkijat pystyvätkin lähettämään väärennetyn sähköpostiviestin, jotta näyttäisi siltä, että se on peräisin Remitlyltä, on viestin oikeellisuus joissain tapauksissa mahdollista selvittää tarkistamalla palautusosoite. Jos kyseisen sähköpostiviestin "Lähettäjä"-rivi on esimerkiksi "remitly-security@hotmail.com" tai "remitly-fraud@msn.com" tai siinä on jonkun muun internet-palveluntarjoajan nimi, on varmaa, että viesti ei ole aito.

5. Tarkista verkkosivuston osoite

Aidoilla Remitly-verkkosivustoilla on aina seuraava verkkotunnus: https://www.remitly.com/

Joskus huijausviestien sisältämä linkki näyttää aidolta Remitly-osoitteelta. Voit tarkistaa, mihin se tosiasiassa osoittaa siirtämällä hiiren kyseisen linkin yläpuolelle – varsinainen verkkosivusto, johon linkki osoittaa, näkyy selainikkunasi alaosan tilapalkissa tai ponnahdusikkunana.

Remitly ei koskaan käytä verkko-osoitteita, joiden verkkotunnus on jotain muuta kuin yllä mainitut. Esimerkiksi verkkotunnusten muunnelmat, kuten "http://security-payments-remitly.com/" tai IP-osoite (numerojono), jota seuraa hakemisto, kuten "http://123.456.789.123/remitly.com/" eivät ole aitoja Remitly-verkkosivustoja.

Joskus huijausviestit on laadittu niin, että minkä tahansa viestin kohdan napsauttaminen siirtää käyttäjän huijausverkkosivustolle. Remitly ei koskaan lähetä sähköpostiviestejä, jotka toimivat näin. Jos vahingossa napsautat tällaista sähköpostiviestiä ja päädyt huijausverkkosivustolle, älä syötä mitään tietoja – sulje vain kyseinen selainikkuna.

6. Jos jokin sähköpostiviesti näyttää epäilyttävältä, siirry suoraan Remitlyn verkkosivustolle

Jos et ole varma, älä napsauta sähköpostiviestissä olevaa linkkiä. Siirry suoraan osoitteeseen https://www.remitly.com/ ja napsauta oikeassa yläkulmassa olevassa valikossa olevaa kohtaa **Oma tili (Your Account)**. Näin näet viimeisimmät ostokset tai voit tarkastella omia tilitietojasi. Jos et pääse sisään omalle tilillesi tai näet jotain epäilyttävää, ilmoita siitä Remitlylle välittömästi.

7. Omien tilitietojen suojaaminen

Jos kuitenkin napsautit huijausviestiä tai epäilyttävää sähköpostiviestiä ja syötit omia Remitly-tilin tietojasi, sinun tulee päivittää salasanasi **välittömästi**. Tämä voidaan tehdä siirtymällä suoraan osoitteeseen https://www.remitly.com/ ja napsauttamalla **Account Settings (Tiliasetukset)**. Napsauta seuraavalla sivulla kohtaa **Change your personal information, e-mail address, or password (Muuta henkilötietoja, sähköpostiosoitetta tai salasanaa)**.

Jos annoit luottokorttinumerosi sivustolla, jonne huijausviesti sinut linkitti, Remitly suosittelee ryhtymistä toimenpiteisiin omien tietojen suojaamiseksi. Kannattaa esimerkiksi ottaa yhteyttä omaan luottokorttiyhtiöön ja ilmoittaa heille tapahtuneesta. Ja lopuksi sinun tulee poistaa kyseinen luottokortti omalta Remitly-tililtäsi, jotta luvaton pääsy tilillesi voidaan estää.

8. Verkkourkintaviesteistä ilmoittaminen

Jos olet saanut sähköpostiviestin, jonka tiedät olevan väärennetty tai jos epäilet olevasi verkkourkintahyökkäyksen uhri ja olet huolissasi omasta Remitly-tilistäsi, kerro asiasta Remitlylle välittömästi ilmoittamalla [verkkourkinta- tai huijaussähköpostiviestistä](https://www.remitly.com/home/contact).