Transaktions- och kontosäkerhet

Kontosäkerhet är viktigt för oss och vi har tagit flera steg för att skydda dina Remitly-konto relaterade uppgifter. Det finns också en del saker du kan göra för att skydda ditt konto och dina personuppgifter.

Kontoverifieringsprocess

Ditt Remitly-konto måste genomgå verifieringsprocedurer för att upprätthålla säkerhet, förtroende och skydd på hög nivå.

Om du är en ny Remitly-kund och skapar ett nytt Remitly-konto på Remitlys webbplats så måste du ange vissa personuppgifter och genomgå mail verfieringsprocessen.

När ditt konto är skapat och fungerar som det ska använder vi en rad olika manuella och automatiska riskhanteringsprocedurer som kan visa på misstänkt kontoaktivitet. Syftet är att identifiera kännetecken som är ovanliga eller inte stämmer överens med ditt tidigare användningsmönster. Som en del av denna process kontaktar vi branschledande tjänsteleverantörer för att verifiera dina personuppgifter och din finansiella information. Dessa tjänsteleverantörer kommer aldrig att kontakta dig direkt eller använda dina uppgifter i något annat syfte än att slutföra din transaktion.

Lösenordsäkerhet

När du loggar in på ditt konto gör vi vissa saker för att skydda ditt konto. Först, när du loggar in på ditt Remitly-konto loggar du in med en säker serveranslutning (https://). Vi använder Secure Socket Layer (SSL) med 256-bit kryptering vilket är industristandarden för säkert serverskydd.

Ditt konto skyddas också av ett unikt lösenord som du själv skapar. Använd inte vanliga ord eller fraser som ditt lösenord. Ditt lösenord ska helst bestå av minst 8 tecken, både siffror och bokstäver med både små och stora bokstäver. Håll detta lösenord hemligt. Om du delar ditt lösenord kommer ditt Remitly-konto att bli mindre säkert.

Se upp för internetsvindleri

- Gör INTE en betalning för att hämta ut en lotteri- eller prisvinst, eller mot ett löfte om att motta en stor summa pengar.
- Gör INTE en betalning eftersom har blivit "garanterad" ett kreditkort eller lån.
- Svara INTE på ett internet- eller telefonerbjudande som du inte är övertygad är äkta.

- Gör INTE en betalning till någon du inte känner och vars identitet du inte kan bekräfta.

Om du är osäker be den avsedda mottagen om mer information om den begärda betalningens syfte och säkerhet. Skicka inte betalningen förrän du är säker på att transaktionen är säker och legitim.

Identifiera nätfiske och förfalskade mail

Det kan hända att du mottar e-post som ser ut att komma från Remitly men som faktiskt är falsk. Sådana mail kan skicka dig direkt till en webbplats som liknar Remitlys webbplats. Du kan till och med bli ombedd att ge ut kontouppgifter, som sin mailadress och lösenord.

Dessa falska webbplatser kan stjäla dina känsliga konto- och betalningsuppgifter för att begå bedrägerier. Dessa falska mail kan innehålla potentiella virus eller malware som kan upptäcka lösenord eller känslig information. Vi rekommenderar därför att du installerar ett antivirusprogram och se till att det alltid är uppdaterat.

Här är några viktiga saker att komma ihåg när det gäller försvar mot falska mail:

1. Remitly kommer inte att be om följande via e-post:

- Ditt fullständiga personnummer eller födelsedatum.
- Ditt kreditkortsnummer, PIN-kod eller säkerhetskoden på ditt kreditkort (inklusive "uppdateringar" av någon av de ovanstående)

2. Se upp för bilagor i misstänkta e-postmeddelanden. Vi rekommenderar att du inte öppnar bilagor från misstänkta eller okända avsändare. Bilagor kan innehålla virus som kan infektera din dator när bilagan öppnas. Om du mottar ett mail som utger sig för att komma från Remitly vilket innehåller en bilaga rekommenderar vi att du raderar mailet utan att öppna bilagan.

3. Håll utkik efter grammatiska eller typografiska misstag

Håll utkik efter dålig grammatik eller typografiska misstag. En del nätfiskemail är översatta eller skickas utan att korrekturläsas och innehåller därför dålig grammatik eller typografiska misstag.

4. Kontrollera avsändaradressen

Är detta e-postmeddelande från Remitly? Även om nätfiskare kan skicka förfalskade mail för att få dem att se ut som att de kommer från Remitly så är det ibland möjligt att avgöra om de är äkta genom att kontrollera avsändaradressen. Om mailets "från" fält ser ut så här "remitly-security@hotmail.com" eller "remitly-fraud@msn.com" eller innehåller namnet på en annan internetleverantör kan du vara helt säker på att det inte är ett äkta mail.

5. Kontroller webbplatsadressen

Äkta Remitly webbplatser har den följande värddomänen: https://www.remitly.com/

Ibland kan länken i det förfalskade mailet se ut som en riktig Remitly-adress. Du kan se vart den faktiskt leder till genom att föra musen över länken -- webbplatsen den faktiskt leder till kommer att visas i statusfältet längst ner på ditt sökmotorfönster eller som ett pop-up-fönster.

Vi använder aldrig en webbadress med en värddomän än de som listas ovan. Till exempel, olika domäner som "http://security-payments-remitly.com/" eller en IP-adress (en sträng med nummer) följd av förteckningar som "http://123.456.789.123/remitly.com/" är inte giltiga Remitly-webbplatser.

Ibland fungerar förfalskade mail så att om du klickar någonstans på texten i mailet kommer du direkt till en falsk webbplats. Remitly kommer aldrig att skicka ett mail som gör detta. Om du av misstag klickar på ett sådant mail och går till en falsk webbplats ange inga uppgifter; stäng istället ner sökmotorfönstret.

6. Gå direkt till Remitlys webbplats om ett mail ser misstänkt ut.

Om du är det minsta osäker klicka inte på länken i mailet. Gå direkt till https://www.remitly.com/ och klicka på **Ditt konto** i menyn i övre högra hörnet för se senaste köp och för att kontrollera dina kontouppgifter. Om du inte kommer åt ditt konto eller om du ser något misstänk så kontakta oss på en gång.

7. Skydda dina kontouppgifter

Om du klickade på en länk i ett förfalskat eller misstänkt mail och du angivit dina

uppgifter från ditt Remitly-konto ska du omedelbart uppdatera ditt lösenord. Du kan göra detta genom att gå direkt till https://www.remitly.com/ och klicka på **Kontoinställningar**. På nästa sida klicka på **Ändra dina personuppgifter, mailadress eller lösenord**.

Om du angivit ditt kreditkortsnummer på webbplatsen länkad till i det förfalskade mailet rekommenderar vi att du tar steg för att skydda dina uppgifter. Det kan också vara en bra ide att t.ex. kontakta din kreditkortsutgivare för att berätta om vad som hänt. Slutligen bör du radera ditt kreditkort från ditt Remitly-konto för att förhindra att någon otillbörligen återfår tillgång till ditt konto.

8. Rapportera nätfiskemail

Om du har fått ett mail som du vet är en förfalskning, eller om du tror att du är utsatt för en nätfiskeattack och du är bekymrad över ditt Remitly-konto meddela oss på en gång genom att rapportera ett [nätfiske- eller förfalskat mail](https://www.remitly.com/home/contact).