Transaksjons- og kontosikkerhet

Kontosikkerhet er viktig for oss og vi har tatt flere grep for å beskytte opplysningene dine knyttet til din Remitly-konto. Du kan også gjøre visse ting som kan hjelpe deg å beskytte kontoen og personopplysningene dine.

Kontoverifiseringsprosesser

Din Remitly-konto er gjenstand for verifiseringsprosedyrer for å opprettholde høye sikkerhetsnivåer, tillit og beskyttelse.

Hvis du er en ny Remitly-kunde og oppretter en ny Remitly-konto ved å bruke Remitlys nettsted, må du oppgi visse personopplysninger og fullføre e-postverifiseringsprosessen.

Når kontoen din er satt opp og aktivert vil vi sende deg visse manuelle og automatiske risikostyringsprosedyrer som lar oss identifisere mistenkelig kontoaktivitet. Målet er å identifisere karakteristikker som ser uvanlige eller inkonsekvente ut sammenlignet med tidligere bruk. Som en del av denne prosessen inngår vi kontrakter med bransjens ledende tjenesteytere for å verifisere personlig og økonomisk informasjon. Disse tjenestene vil aldri kontakte deg direkte eller benytte dine opplysninger for noe annet enn gjennomføring av den tiltenkte transaksjonen.

Passordsikkerhet

Når du logger på kontoen gjør vi en del ting for å beskytte kontoen din. Når du logger på Remitly-kontoen din, logger du på med en sikker servertilkobling (https://). Vi bruker Secure Socket Layer (SSL) med en 256-bitkryptering, indstristandarden i sikker serverbeskyttelse.

Kontoen din er også beskyttet av et unikt passord som du lager. Du bør ikke bruke vanlige ord eller setninger i passordet ditt. I stedet bør passordet ditt være minst åtte tegn, inkludert både tall og bokstaver ved å bruke store og små bokstaver. Du bør holde passordet konfidensielt. Det å dele passordet ditt vil forringe sikkerheten til din Remitly-konto.

Vær obs på nettsvindel

- IKKE betal for å motta lotteri- eller premiegevinster, eller mot et løfte om å motta en stor sum penger.
- IKKE betal fordi du «garanterer» et kredittkort eller lån.
- IKKE besvar et tilbud på Internett eller telefonen som du ikke er sikker på om

er et reellt tilbud.

- IKKE betal til noen du ikke kjenner eller hvis identitet du ikke kan bekrefte.

Når du er i tvil, må du be den tiltenkte mottakeren om mer informasjon om formål og sikkerheten til den anmodede betalingen. Ikke send betalingen før du er komfortabel med transaksjonen.

Identifisere phishing eller falske e-poster

Du kan samtidig motta e-poster som ser ut som de kom fra Remitly, men som faktisk er falske. Slike e-poster kan omdirigere deg til et nettsted som ligner på Remitlys nettsted. Du kan også bli bedt om å oppgi kontoopplysninger som e-postadresse og passord.

Disse falske nettstedene kan stjele sensitive opplysninger og betalingsinformasjon for å begå svindel. Disse falske e-postene kan inneholde mulige virus eller ondsinnet programvare som kan stjele passord eller sensitive opplysninger. Vi anbefaler derfor at du installerer et antivirusprogam og holder det oppdatert til enhver tid.

Her er noen sentrale punkter å huske på for å forsvare deg mot falske e-poster:

1. Kjenn til det Remitly ikke vil be om på e-post

- Hele personnummeret ditt eller fødselsdato
- Kredittkortnummeret, PIN-kode eller kredittkortets sikkerhetskode (inkludert «oppdateringer» for noe av de ovennevnte)
- **2. Vær obs på vedlegg i mistenkelige e-poster**

Vi anbefaler at du ikke åpner e-postvedlegg fra mistenkelige eller ukjente kilder. E-postvedlegg kan inneholde virus som infiserer datamaskinen din når vedlegget åpnes. Hvis du mottar mistenkelige e-poster som synes å være sendt fra Remitly og som inneholder et vedlegg, anbefaler vi at du sletter e-posten uten å åpne vedlegget.

3. Se etter grammatikk eller stavefeil

Se etter dårlig grammatikk eller stavefeil. Noen Phishing-e-poster oversettes fra andre språk eller sendes uten å korrekturleses, og inneholder følgelig dårlig grammatikk eller stavefeil.

4. Sjekk avsenderadressen

Kommer denne e-posten fra Remitly? Mens phishere kan sende en falsk e-post som ser ut som den kommer fra Remitly, kan du noen ganger se om den er ekte ved å sjekke avsenderadressen. Hvis «fra»-linjen i e-posten har følgende innhold «remitly-security@hotmail.com» eller «remitly-fraud@msn.com», eller inneholder navnet på en annen nettleverandør, kan du være skråsikker på at den er falsk.

5. Sjekk nettsidens adresse

Ekte nettsider fra Remitly bruker alltid servere med følgende domene: https://www.remitly.com/

Noen ganger vil lenken i falske e-poster se ut som en ekte Remitly-adresse. Du kan sjekke hvor den faktisk leder til ved å føre musepekeren over lenken – den faktiske nettsiden hvor den peker til vil vises i statuslinjen øverst i nettleserens vindu eller som en pop-up.

Vi vil aldri ha benyttet nettadressen fra et domene utover de oppgitt over. For eksempel kan det være variasjoner av domenet, som «https://security-payments-remitly.com/» eller en IP-adresse (tallrekke) etterfulgt av kataloger som «https://123.456.789.123/remitly.com/» er ikke gyldige Remitly-nettsider.

Videre vil visse falske e-poster også sette det opp slik at du omdirigeres til den falske nettsiden uansett hvor du klikker. Remitly vil aldri sende e-poster som gjør dette. Hvis du klikker på en slik lenke og kommer til den falske nettsiden, må du ikke oppgi informasjon; i stedet må du lukke vinduet.

6. Hvis en e-post ser mistenkelig ut, bør du gå direkte til Remitlys nettsted

Hvis du er i tvil, må du ikke klikke på lenken i e-posten. Gå direkte til https://www.remitly.com/ og klikke **Din konto** i menyen øverst til høyre til nylige kjøp, eller se over kontoopplysningene dine. Hvis du ikke får tilgang til kontoen din, eller hvis du ser noe mistenkelig, bør du melde fra til oss om dette umiddelbart.

7. Beskytt kontoopplysningene dine

Hvis du klikker deg gjennom en falsk nettside eller mistenkelige e-poster, og du har oppgitt dine Remitly-kontoopplysninger, bør du oppdatere passordet ditt **umiddelbart**. Du kan gjøre dette ved å gå direkte til https://www.remitly.com/ og klikke på **Kontoinnstillinger**. På neste side må du klikke **Endre personopplysninger, e-postadresse eller passord**.

Hvis du har tastet inn kredittkortnummeret ditt på nettsiden med lenke fra den falske e-postmeldingen, anbefaler vi at du tar grep for å beskytte informasjonen din. Du bør kanskje, for eksempel, kontakte kredittkortselskapet for å varsle dem om dette. Til slutt bør du slette kredittkortet fra Remitly-kontoen din for å forhindre at noen får uautorisert tilgang til kontoen din.

8. Rapportering av phishing e-post

Hvis du har mottatt en e-post du vet er falsk, eller hvis du mener du har vært et offer for et phishing-angrep og du er bekymret for Remitly-kontoen din, må du fortelle oss dette umiddelbart ved å rapportere en [phishing eller falsk e-post](https://www.remitly.com/no/no/home/contact).