Transaktions- og kontosikkerhed

Kontosikkerhed er vigtig for os, og vi har truffet adskillige foranstaltninger for at beskytte dine Remitly-kontorelaterede oplysninger. Du kan også gøre visse ting, der kan hjælpe med at beskytte din konto og dine personoplysninger.

Kontobekræftelsesprocesser

Din Remitly-konto er underlagt bekræftelsesprocesser for at opretholde et højt niveau af sikkerhed, tillid og beskyttelse.

Hvis du er ny Remitly-kunde, og du opretter en ny Remitly-konto gennem Remitlys websted, skal du tilvejebringe visse personoplysninger og gennemføre e-mailbekræftelsen.

Når din konto er oprettet, implementerer vi en række manuelle og automatiserede risikostyringsprocedurer, der gør det muligt for os at fremhæve mistænkelig kontoaktivitet. Målet er at identificere eventuelle egenskaber, der virker usædvanlige eller uforenelige med din tidligere brug. Som led i denne proces samarbejder vi med brancheførende tjenesteudbydere for at bekræfte personoplysninger og finansielle oplysninger. Disse tjenester vil aldrig kontakte dig direkte eller bruge dine oplysninger til andet end den vellykkede gennemførelse af din påtænkte transaktion.

Adgangskodesikkerhed

Når du logger ind på din konto, gør vi visse ting for at beskytte din konto. For det første, når du logger ind på din Remitly-konto, logger du ind ved hjælp af en sikker serverforbindelse (https://). Vi bruger secure socket layer (SSL) med 256-bit kryptering, branchestandarden inden for sikker serverbeskyttelse.

Din konto beskyttes også af en unik adgangskode, som du opretter. Du bør ikke bruge almindelige ord eller sætninger som din adgangskode. Din adgangskode skal i stedet være mindst otte tegn, herunder både tal og store og små bogstaver. Du bør holde denne adgangskode fortrolig. Deling af din adgangskode mindsker sikkerheden af din Remitly-konto.

Vær opmærksom på internetsvindel

- Foretag IKKE en betaling for at indløse lotterigevinster eller præmier eller for et løfte om at modtage en stor sum penge.
- Foretag IKKE en betaling, fordi du er "garanteret" et kreditkort eller et lån.
- Svar IKKE på et internet- eller telefontilbud, som du ikke er sikker på, er ærligt.

- Foretag IKKE en betaling til en person, som du ikke kender, eller hvis identitet du ikke kan bekræfte.

Hvis du er i tvivl, skal du bede den påtænkte modtager om flere oplysninger om formålet med og sikkerheden af den anmodede betaling. Send ikke betalingen, før du er tryg ved transaktionen.

Identifikation af phishing- eller falske e-mails

Du kan på et eller andet tidspunkt modtage en e-mail, der ser ud som om, at den kom fra Remitly, men rent faktisk ikke er ægte. En sådan e-mail kan henvise dig til et websted, der ligner Remitly-webstedet. Du kan endda blive bedt om at tilvejebringe kontooplysninger såsom din e-mailadresse og adgangskode.

Disse falske websteder kan stjæle dine følsomme konto- og betalingsoplysninger med henblik på at begå svig. Disse falske e-mails kan indeholde potentielle vira eller malware, der kan registrere adgangskoder eller følsomme oplysninger. Vi anbefaler derfor, at du installerer et antivirusprogram og til enhver tid holder det opdateret.

Her er nogle nøglepunkter, som du skal huske som en del af et forsvar mod svigagtige e-mails:

1. Du skal vide, hvad Remitly ikke vil bede om via e-mail

- Dit fulde CPR-nummer eller din fødselsdato
- Dit kreditkortnummer, din pinkode eller dit kreditkorts sikkerhedskode (herunder "opdateringer" af enhver af ovenstående)

2. Pas på vedhæftede filer i mistænkelige e-mails

Vi anbefaler, at du ikke åbner vedhæftede filer i e-mails fra mistænkelige eller ukendte kilder. Vedhæftede filer i e-mails kan indeholde vira, der inficerer din computer, når den vedhæftede fil åbnes. Hvis du modtager en mistænkelig e-mail, der angiveligt er sendt fra Remitly, der indeholder en vedhæftet fil, anbefaler vi, at du sletter e-mailen uden at åbne den vedhæftede fil.

3. Hold øje med grammatiske eller typografiske fejl

Hold øje med dårlig grammatik eller typografiske fejl. Nogle phishing-e-mails oversættes fra andre sprog eller sendes uden at blive korrekturlæst, og som følge heraf

indeholder de dårlig grammatik eller typografiske fejl.

4. Kontrollér returadressen

Er e-mailen fra Remitly? Selv om phishere kan sende en falsk e-mail for at få det til at se ud som om, at den kom fra Remitly, kan du nogle gange se, hvorvidt den er autentisk, ved at tjekke returadressen. Hvis "fra"-linjen i e-mailen ligner "remitly-security@hotmail.com" eller "remitly-fraud@msn.com" eller indeholder navnet på en anden internettjenesteudbyder, kan du være sikker på, at den ikke er ægte.

5. Kontrollér webstedets adresse

Ægte Remitly-websteder hostes altid på det følgende domæne: https://www.remitly.com/

Sommetider ligner linket i falske e-mails en ægte Remitly-adresse. Du kan kontrollere, hvor det rent faktisk peger hen, ved at køre musen over linket – det egentlige websted, som det peger, på vises i statuslinjen nederst i dit browservindue eller som en pop-up.

Vi bruger aldrig en webadresse, der hostes på et andet domæne end dem, der er angivet ovenfor. For eksempel forskellige domæner såsom "https://security-payments-remitly.com/" eller en IP-adresse (talstreng) efterfulgt af registre såsom "https://123.456.789.123/remitly.com/" er ikke gyldige Remitly-websteder.

Sommetider er den falske e-mail oprettet således, at hvis du klikker hvor som helst på teksten, bliver du dirigeret til det svigagtige websted. Remitly vil aldrig sende en e-mail, der gør dette. Hvis du klikker på en sådan e-mail ved et uheld og går til et falsk websted, skal du ikke indtaste nogen oplysninger. I stedet skal du bare lukke det pågældende browservindue.

6. Hvis en e-mail ser mistænkelig ud, skal du gå direkte til Remitly-webstedet

Hvis du er i tvivl, skal du ikke klikke på linket, der indgår i en e-mail. Gå direkte til https://www.remitly.com/, og klik på **Din Konto** i øverste højre menu for at se de seneste køb eller gennemgå dine kontooplysninger. Hvis du ikke kan få adgang til din konto, eller hvis du ser noget mistænkeligt, skal du omgående underrette os.

7. Beskyt dine kontooplysninger

Hvis du klikkede igennem fra en falsk eller mistænkelig e-mail, og du indtastede dine Remitly-kontooplysninger, skal du **omgående** opdatere din adgangskode. Du kan gøre dette ved at gå direkte til https://www.remitly.com/ og klikke på **Kontoindstillinger**. På den næste side, skal du klikke på ***Ændr dine personoplysninger, e-mailadresse eller adgangskode***.

Hvis du har indsendt dit kreditkortnummer til webstedet, hvortil der linkes fra den falske e-mailmeddelelse, anbefaler vi, at du træffer foranstaltninger for at beskytte dine oplysninger. Du bør muligvis kontakte for eksempel dit kreditkortselskab for at underrette dem om denne sag. Endelig skal du slette det pågældende kreditkort fra din Remitly-konto for at forhindre andre personer i uretmæssigt at tilegne sig adgang til din konto.

8. Indberetning af phishing-e-mail

Hvis du har modtaget en e-mail, som du ved er falsk, eller hvis du mener, at du er blevet offer for et phishingangreb, og du er bekymret for din Remitly-konto, skal du omgående underrette os ved at indberette en [phishing- eller falsk e-mail](https://www.remitly.com/dk/da/home/contact).