লেনদেন ও অ্যাকাউন্টের সুরক্ষা

অ্যাকাউন্টের সুরক্ষা আমাদের কাছে গুরুত্বপূর্ণ এবং আমরা আপনার Remitly অ্যাকাউন্ট-সম্পর্কিত তথ্য সুরক্ষিত রাখতে বেশ কিছু পদক্ষেপ নিয়েছি। আপনি নিজেও কিছু কিছু কাজ করতে পারেন যা আপনার অ্যাকাউন্ট এবং ব্যক্তিগত তথ্য সুরক্ষিত করতে সাহায্য করবে।

অ্যাকাউন্ট যাচাইকরণ প্রতিক্রিয়া

উচ্চ স্তরের নিরাপত্তা, বিশ্বাস এবং সুরক্ষা বজায় রাখতে আপনার Remitly অ্যাকাউন্টটি যাচাইকরণ পদ্ধতির অধীনে থাকে।

আপনি যদি একজন নতুন Remitly গ্রাহক হন এবং আপনি Remitly ওয়েবসাইট ব্যবহার করে একটি নতুন Remitly অ্যাকাউন্ট তৈরি করেন, তাহলে আপনাকে অবশ্যই কিছু ব্যক্তিগত তথ্য প্রদান করতে হবে এবং ইমেল যাচাইকরণ প্রক্রিয়া সম্পূর্ণ করতে হবে।

একবার আপনার অ্যাকাউন্ট চালু হয়ে গেলে আমরা বিভিন্ন ধরনের ম্যানুয়াল এবং স্বয়ংক্রিয় ঝুঁকি ব্যবস্থাপনা পদ্ধতি প্রয়োগ করি, যার ফলে সন্দেহজনক অ্যাকাউন্টের কার্যকলাপের উপর আমরা দৃষ্টি নিবদ্ধ করতে পারি। লক্ষ্য হল আপনার অতীত ব্যবহারের সাথে অস্বাভাবিক বা অসামঞ্জস্যপূর্ণ বলে মনে হয় এমন কোনো বৈশিষ্ট্যকে চিহ্নিত করা। এই প্রক্রিয়ার অংশ হিসাবে আমরা ব্যক্তিগত এবং আর্থিক তথ্য যাচাই করার জন্য শিল্পের শীর্ষস্থানীয় পরিষেবা প্রদানকারীদের সাথে চুক্তি করে থাকি। আপনার উদ্দেশ্যমূলক লেনদেনের সফল সমাপ্তি ছাড়া অন্য কিছুর জন্য এই পরিষেবাগুলি কখনোই আপনার সাথে সরাসরি যোগাযোগ করবে না বা আপনার তথ্য ব্যবহার করবে না।

পাসওয়ার্ড সুরক্ষা

আপনি যখন আপনার অ্যাকাউন্টে লগ ইন করেন আমরা আপনার অ্যাকাউন্ট সুরক্ষিত করার জন্য কিছু করি। প্রথমত, আপনি যখনই আপনার Remitly অ্যাকাউন্টে লগ ইন করবেন, আপনি একটি সুরক্ষিত সার্ভার সংযোগ (https://) ব্যবহার করে লগ ইন করবেন। সুরক্ষিত সার্ভার সুরক্ষায় আমরা শিল্পের স্ট্যান্ডার্ড মানের 256-বিট এনক্রিপশন সহ সিকিউর সকেট লেয়ার (SSL) ব্যবহার করি।

এছাড়াও আপনার অ্যাকাউন্ট আপনার তৈরি করা একটি স্বতন্ত্র পাসওয়ার্ড দ্বারা সুরক্ষিত থাকে। আপনার

পাসওয়ার্ডের জন্য পরিচিত শব্দ বা বাক্যাংশ ব্যবহার করা উচিত নয়। বরং, আপনার পাসওয়ার্ডটি কমপক্ষে আটটি বর্ণের হওয়া উচিত যার মধ্যে সংখ্যা এবং বড় হাতের ও ছোট হাতের অক্ষর উভয়ই থাকা উচিত। আপনার এই পাসওয়ার্ডটি গোপন রাখা উচিত। আপনার পাসওয়ার্ড শেয়ার করলে তা আপনার Remitly অ্যাকাউন্টের সুরক্ষাকে কমিয়ে দেবে।

ইন্টারনেটের বিভিন্ন প্রতারণা সম্পর্কে সতর্ক থাকুন

কোনো লটারি বা পুরস্কার জেতার দাবির পরিপ্রেক্ষিতে অথবা অনেক বেশি পরিমাণ টাকা পাওয়ার প্রতিশ্রুতিতে বিশ্বাস করে কোনো পেমেন্ট করবেন না।

আপনাকে ক্রেডিট কার্ড বা ঋণের "নিশ্চয়তা" দেওয়া হয়েছে এই কারণে কোনো পেমেন্ট করবেন না।

ইন্টারনেট বা ফোনের মাধ্যমে করা এমন কোনো অফারের উত্তর দেবেন না, যা আপনার বিশ্বাসযোগ্য বলে মনে হচ্ছে না।

এমন কাউকে পেমেন্ট করবেন না যাকে আপনি চেনেন না অথবা যার পরিচয় আপনি যাচাই করতে পারছেন না।

সন্দেহ হলে, অনুরোধকৃত পেমেন্টের উদ্দেশ্য এবং সুরক্ষা সংক্রান্ত আরও তথ্যের জন্য উদ্দিষ্ট প্রাপককে জিজ্ঞাসাবাদ করুন। আপনি লেনদেনটিতে স্বচ্ছন্দ না হওয়া পর্যন্ত পেমেন্ট করবেন না।

ফিশিং বা জাল ইমেল চিহ্নিত করা

আপনি কখনও কখনও এরকম ইমেল পেতে পারেন, যা দেখে মনে হতে এটি Remitly থেকে এসেছে, কিন্তু প্রকৃতপক্ষে এটি আসল নয়। এই ধরনের একটি ইমেল আপনাকে Remitly ওয়েবসাইটের মতো দেখতে একটি ওয়েবসাইটের দিকে নির্দেশিত করতে পারে। এমনকি আপনাকে আপনার ইমেল ঠিকানা এবং পাসওয়ার্ডের মতো অ্যাকাউন্টের বিবরণ প্রদান করতে বলা হতে পারে।

এই জাল ওয়েবসাইটগুলি প্রতারণা করার জন্য আপনার অ্যাকাউন্ট এবং পেমেন্টের সংবেদনশীল তথ্য চুরি করতে পারে। এই জাল ইমেলগুলিতে সম্ভাব্য ভাইরাস বা ম্যালওয়্যার থাকতে পারে, যা পাসওয়ার্ড বা সংবেদনশীল

তথ্যকে চিহ্নিত করতে পারে। তাই আমরা সুপারিশ করি যে, আপনি একটি অ্যান্টি-ভাইরাস প্রোগ্রাম ইনস্টল করুন এবং এটিকে সর্বদা আপডেট রাখুন।

প্রতারণামূলক ইমেলের বিরুদ্ধে সুরক্ষার অংশ হিসেবে এখানে কিছু মূল বিষয় মাথায় রাখতে হবে:

জেনে রাখুন যে, Remitly ইমেলের মাধ্যমে এগুলি চাইবে না

আপনার সম্পূর্ণ সোশ্যাল সিকিউরিটি নম্বর ও জন্মতারিখ

আপনার ক্রেডিট কার্ড নম্বর, PIN, ক্রেডিট কার্ড সিকিউরিটি কোড (এর মধ্যে রয়েছে উপরোক্ত কোনো একটির "আপডেট")

সন্দেহজনক ইমেলের অ্যাটাচমেন্টের বিষয়ে সতর্ক থাকুন

আমরা পরামর্শ দিচ্ছি যে, সন্দেহজনক বা অজানা উৎস থেকে আসা কোনো ইমেল অ্যাটাচমেন্ট খুলবেন না। ইমেল অ্যাটাচমেন্টে ভাইরাস থাকতে পারে এবং এই অ্যাটাচমেন্ট খোলা হলে আপনার কম্পিউটার সংক্রমিত হতে পারে। আপনি যদি Remitly থেকে প্রেরিত সন্দেহজনক ইমেল পান, যেটিতে একটি অ্যাটাচমেন্ট রয়েছে, আমরা সুপারিশ করি যে, আপনি অ্যাটাচমেন্টটি না খুলেই ইমেলটিকে মুছে ফেলুন।

কোনো ব্যাকরণগত বা টাইপে ভুল আছে কিনা দেখুন

ভুল ব্যাকরণ বা টাইপের ত্রুটি আছে কিনা দেখুন। কিছু ফিশিং ইমেল অন্য ভাষা থেকে অনুবাদ করা হয় বা প্রুফরিড করা ছাড়াই পাঠানো হয় এবং ফলস্বরূপ, এর ব্যাকরণে ভুল থাকে বা টাইপের ত্রুটি থাকে।

ফেরত পাঠানোর ঠিকানাটি যাচাই করুন

[ইমেলটি কি Remitly থেকে এসেছে? যদিও ফিশিংকারীরা এরকম একটি জাল ইমেল পাঠাতে পারে যা Remitly থেকে এসেছে বলে মনে হবে, আপনি কখনও কখনও ফেরত পাঠানোর ঠিকানা যাচাই করে

এটি আসল কিনা তা নির্ধারণ করতে পারেন। যদি ইমেলের "ফ্রম" লাইনটি "remitly-security@hotmail.com" বা "remitly-fraud@msn.com"-এর মতো দেখায় বা অন্য ইন্টারনেট পরিষেবা প্রদানকারীর নাম থাকে, তাহলেও আপনি নিশ্চিত হতে পারেন যে এটি আসল নয়।](mailto:remitly-security@hotmail.com)

ওয়েবসাইটের ঠিকানাটি যাচাই করুন

[আসল Remitly ওয়েবসাইটগুলি সর্বদা নিম্নলিখিত ডোমেইনে হোস্ট করা হয়: https://www.remitly.com/](https://www.remitly.com/)

কখনও কখনও জালিয়াতি করা ইমেলে থাকা লিঙ্কটি একটি আসল Remitly ঠিকানার মত দেখায়। আপনি লিঙ্কের উপর আপনার মাউস ঘুরিয়ে এটি আসলে কোথায় নির্দেশিত করছে তা পরীক্ষা করতে পারেন - এটি যে আসল ওয়েবসাইট নির্দেশ করে তা আপনার ব্রাউজার উইন্ডোর নিচের স্ট্যাটাস বারে বা একটি পপ-আপ হিসাবে দেখানো হবে।

[আমরা কখনোই উপরে তালিকাভুক্ত ডোমেইনে হোস্ট করা ওয়েব ঠিকানা ব্যবহার করি না। উদাহরণস্বরূপ, ভ্যারিয়েন্ট ডোমেইন যেমন "https://security-payments-remitly.com/…।" অথবা "https://123.456.789.123/remitly.com/…"-এর মতো ডিরেক্টরির পরে থাকা একটি IP ঠিকানা (নম্বরের স্ট্রিং) সঠিক Remitly ওয়েবসাইট নয়।](https://security-payments-remitly.com/)

এছাড়াও, কখনও কখনও জালিয়াতি করা ইমেলটি এমনভাবে সেট আপ করা হয়, যে আপনি টেক্সটটির কোথাও ক্লিক করলে আপনাকে জাল ওয়েবসাইটে নির্দেশিত করা হবে। Remitly কখনোই এরকম ইমেল পাঠায় না। আপনি যদি ভুলবশত এই ধরনের একটি ইমেলে ক্লিক করেন এবং একটি জাল ওয়েবসাইটে যান, কোনো তথ্য লিখবেন না; বরং, শুধু সেই ব্রাউজার উইন্ডোটি বন্ধ করুন।

যদি একটি ইমেল সন্দেহজন দেখায়, সরাসরি Remitly ওয়েবসাইটে যান

[সন্দেহ হলে, ইমেল থাকা লিঙ্কে ক্লিক করবেন না। সরাসরি https://www.remitly.com/-এ যান এবং সাম্প্রতিক কেনাকাটা দেখতে বা আপনার অ্যাকাউন্টের তথ্য পর্যালোচনা করতে উপরের ডানদিকের

মেনুতে আপনার অ্যাকাউন্টে ক্লিক করুন। আপনি যদি আপনার অ্যাকাউন্ট অ্যাক্সেস করতে না পারেন, বা আপনি যদি সন্দেহজনক কিছু দেখতে পান, তাহলে এখনই আমাদের জানান।](https://www.remitly.com/)

আপনার অ্যাকাউন্টের তথ্য সুরক্ষিত রাখুন

[আপনি যদি জাল বা সন্দেহজনক ইমেলের মাধ্যমে ক্লিক করেন এবং আপনি আপনার Remitly অ্যাকাউন্টের তথ্য লেখেন, তাহলে আপনাকে অবিলম্বে আপনার পাসওয়ার্ড আপডেট করতে হবে। আপনি সরাসরি https://www.remitly.com/-এ গিয়ে অ্যাকাউন্ট সেটিংসে ক্লিক করে তা করতে পারেন। পরবর্তী পেজে, আপনার ব্যক্তিগত তথ্য, ইমেল ঠিকানা, বা পাসওয়ার্ড পরিবর্তন করুন-এ ক্লিক করুন।](https://www.remitly.com/)

আপনি যদি জাল ইমেল মেসেজ থেকে লিঙ্ক করা সাইটে আপনার ক্রেডিট কার্ড নম্বরটি লেখেন, তাহলে আমরা আপনাকে আপনার তথ্য সুরক্ষিত করার জন্য পদক্ষেপ নেওয়ার পরামর্শ দেবো। আপনি আপনার ক্রেডিট কার্ড কোম্পানির সাথে যোগাযোগ করতে চাইতে পারেন, উদাহরণস্বরূপ, তাদেরকে এই বিষয়ে জানাতে। পরিশেষে, আপনার অ্যাকাউন্টে বেঠিকভাবে পুনরায় অ্যাক্সেস পাওয়ার থেকে কাউকে আটকাতে, আপনার Remitly অ্যাকাউন্ট থেকে সেই ক্রেডিট কার্ডটি মুছে ফেলা উচিত।

ফিশিং ইমেল সম্পর্কে রিপোর্ট করা

[আপনি যদি এমন ইমেল পেয়ে থাকেন, যা আপনি জানেন জাল, অথবা আপনি যদি মনে করেন যে, আপনি ফিশিং আক্রমণের শিকার হয়েছেন এবং আপনি আপনার Remitly অ্যাকাউন্ট সম্পর্কে উদ্বিগ্ন হন, তাহলে অনুগ্রহ করে ফিশিং বা জাল করা ইমেল সম্পর্কে রিপোর্ট করার মাধ্যমে অবিলম্বে আমাদের তা জানান।](https://www.remitly.com/jp/bn/home/contact/)