

«Вы скоро обогатитесь, но сначала подскажите конфиденциальные данные»

Наталья, Нижневартоск

Мне позвонили и представились сотрудником FinCoNet — международная организация, членами которой являются надзорные органы двадцати двух стран в том числе Россия.

Сотрудник представился как Жанна Брагина и сказала, что юридическая компания из офшорной зоны по доверенности оформленной на мое имя, совершает перевод денежных средств со счета брокерской компании на мой счет в размере 8240 евро.

Данная доверенность отправлена Центробанком РФ на допроверку в организацию FinCoNet, так как достоверность сведений в доверенности показалась сомнительной, а в последнее время участились случаи мошенничества по подобным переводам.

Прошу подтвердить достоверность данной информации и подтвердить наличие данного сотрудника.

Совет эксперта по противодействию мошенничеству:

Это типичный пример мошенничества от имени реально существующей организации. В данном случае — от лица международной организации по защите прав потребителей финансовых услуг FinCoNet. На самом деле она не работает с потребителями напрямую, поэтому ее настоящие сотрудники не могли звонить Наталье.

Скорее всего, злоумышленник нашел ФИО и номер телефона Натальи в открытых источниках. Под предлогом «проверки доверенности» для «перевода в несколько тысяч евро» мошенник надеялся выведать у нее персональные данные.

Обычно злоумышленников интересует секретная информация по банковской карте (срок действия, CVV/CVC-коды), которая позволит им украсть деньги со счета доверчивого собеседника. Также телефонные мошенники могут попросить данные паспорта, а затем втайне оформить на него кредит.

Мошенники рассчитывают, что названия авторитетных организаций собьют человека с толку, а радостная новость о скором переводе на крупную сумму — усыпит бдительность.

Чтобы не дать злоумышленникам обогатиться за ваш счет, всегда следуйте правилам финансовой безопасности:

- Никому ни под каким предлогом не диктуйте секретные данные: только мошенники просят назвать коды с обратной стороны банковской карты, ПИН-коды и пароли из СМС от банка.

- Никогда не делитесь персональной информацией о ваших банковских счетах и других финансовых активах с незнакомыми людьми или делайте это по договору, где будут указаны условия использования таких данных. Ни в коем случае не отправляйте копии своих документов компаниям, с которыми вы раньше не имели дела, пока не проверите информацию о них.

- Если вам звонят от имени Банка России или ссылаются на регулятора, позвоните на горячую линию и сообщите об этом: 8-800-300-3000. Вы также можете запросить информацию или пожаловаться на мошенников через интернет-приемную регулятора.

Во всех случаях, когда вы сталкиваетесь с финансовыми мошенниками, пишите заявление в полицию.