

ПРОТОКОЛ №4

совещание с коллективом РГП на ПХВ «Национальный научный центр фтизиопульмонологии РК» МЗ РК

г.Алматы

22.07.2024 г.

Председатель: Рыскулов Г.П. –И.о. заместителя директора

Присутствовали: Руководители структурных подразделений и коллектив
ННЦФ РК.

ПОВЕСТКА ДНЯ:

1. Как не стать жертвой мошенников.
2. Правила, которые помогут обезопасить себя от финансовых потерь.
- 3.Телефонное мошенничество с использованием личных документов

жертвы:

Докладчик Жайнаков М.Б.- комплаенс-офицер.

Выступил Жайнаков М.Б:

Устойчивые способы мошеннических действий:

Вам предлагают оформить на себя кредит, посредством мессенджера «WhatsApp», сообщают, что свяжется работник с правоохранительных органов (ДКНБ, МВД, ДВД, ДП и т.д.) о требовании произвести денежную транзакцию на другие лицевые счета, мошенники посредством мессенджера «WhatsApp» направляют поддельные документы, т.е. постановление о проведении досудебных следственных мероприятий, связываются посредством видеозвонков. Ни в коем случае не соглашайтесь на их условия. Под предлогом поступившего сигнала о несанкционированной операции по карте просит сообщить реквизиты карты, а также SMS-коды. В создаваемой стрессовой ситуации, телефонные мошенники ведут себя достаточно убедительно, не оставляя времени потенциальной жертве для анализа происходящего разговора. Номера телефонов мошенники обычно получают из открытых источников – собирают в социальных сетях, находят в объявлениях.

В таких случаях важно:

- 1) Ни при каких обстоятельствах никому и никогда не сообщайте код из SMS-сообщения, он необходим только для осуществления платежей и переводов
- 2) Входящий номер телефона может совпадать с номерами телефонов руководства и работников Центра, это может быть замаскированный звонок с помощью IP-телефонии из-за границы.
- 3) Не рекомендуется размещать свой личный номер телефона на общедоступном сайте или в социальных сетях.

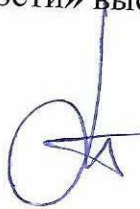
- 4) В случае любых подозрений и сомнений прервите разговор и сами перезвоните в приемную Директора или доложите своему непосредственному руководителю и сообщите о том, что поступил звонок по указанному телефону.
- 5) Так же мошенники могут позвонить под видом Директора, Заместителей (используя специальные программы искусственного интеллекта, которые способны искажать голоса таким образом, чтобы они максимально напоминали голоса руководителей.). Руководство центра не запрашивают конфиденциальную информацию. Немедленно прекратите разговор.
- 6) Никому не сообщайте 3-значный код на обратной стороне банковской карты. Не храните PIN-код рядом с картой. Если вы потеряли карту, обратитесь в свой банк / заблокируйте ее.

Пошаговая инструкция если с Вами связался мошенник:

- 1) Не паникуйте, сохраняйте спокойствие.
- 2) В случае представления сотрудниками с правоохранительных органов (ДКНБ, МВД, ДВД, ДП и т.д.), сообщите о том, что **Вы обратитесь непосредственно в данный правоохранительный орган и немедленно прервите разговор.**
- 3) Не сообщайте никакую информацию о себе и не отвечайте на поставленные вопросы, не поддавайтесь угрозам и давлению со стороны мошенников.
- 4) Прервать разговор и заблокировать мошенника.

И.о. заместителя директора Рыскулов Г.П. «Коллеги киберпреступники становятся изобретательнее в своих подходах, поэтому нужно соблюдать особые меры предосторожности» выступил в заключении.

Председатель



Рыскулов Г.П.