

РЕКОМЕНДУЕМАЯ ПАМЯТКА

о порядке действий при обнаружении признаков мошенничества в отношении работников государственных учреждений Омской области, подведомственных Министерству здравоохранения Омской области (далее – подведомственные учреждения), совершаемого с использованием (применением) информационно-телекоммуникационных технологий, средств телефонной связи или в сфере компьютерной информации (фишинговых (поддельных) сайтов, рассылки сообщений без согласия получателя, размещения опасных вредоносных ссылок и прочего) (далее – дистанционные мошенничества)

Злоумышленники постоянно изменяют формы и методы совершения дистанционных мошенничеств, в том числе ими практикуются телефонные обращения к работникам подведомственных учреждений о переводе денежных средств мошенникам (включая переводы на «безопасные» счета), получении кредитов в банках с целью дальнейшего перевода заемных денежных средств мошенникам, а также руководителям организаций с информацией о предстоящих проверках контрольно-надзорных органов, органов исполнительной власти или вышестоящих организаций и предложением повлиять на их результаты с помощью «вознаграждения» или подарков проверяющим.

При обращении к гражданам мошенники часто представляются должностными лицами органов государственной власти, правоохранительных органов.

В телефонном разговоре мошенники:

1) могут ссылаться на имеющиеся предварительные договоренности с руководством подведомственного учреждения, наличие поручений должностных лиц органов власти, называя персональные данные реальных лиц;

2) ограничивают сроки выполнения поставленной «задачи», исполнения «поручения», подчеркивая, что для их реализации необходимо принятие оперативных мер, выходящих за рамки действующих должностных инструкций;

3) заверяют, что в последующем понесенные при выполнении «поручения» издержки и затраты будут компенсированы;

4) подключают к разговору других лиц, участвующих в мошенничестве и выдающих себя за сотрудников правоохранительных, контрольно-надзорных органов, коллег, руководителей и иных лиц;

5) демонстрируют осведомленность в вопросах организации антитеррористической защищенности объектов, обеспечения противопожарной безопасности, специфики деятельности конкретной организации.

В связи с изложенным предлагается при обнаружении признаков телефонного мошенничества:

- 1) не отвечать на подозрительные телефонные номера;
- 2) в случае, если вызов принят, письменно зафиксировать фамилию, имя, отчество (при наличии), должность звонившего, содержание телефонного разговора;
- 3) уточнить у звонившего номер(а) телефона(ов) обратной связи, но не звонить по ним;
- 4) осуществить аудиозапись телефонного разговора (при наличии технической возможности) и обеспечить ее сохранение;
- 5) завершить телефонный разговор, не сообщая о себе никакой информации;
- 6) по возможности по официальным каналам связи получить от руководителей подведомственных учреждений, должностных лиц органов власти, правоохранительных органов, называемых в разговоре, подтверждение либо опровержение поступившей информации;
- 7) доложить непосредственному руководителю о факте поступления телефонного звонка и его содержание;
- 8) при выдвижении со стороны звонившего преступных требований по переводу денежных средств, приобретения подарков и прочему направить сообщение в территориальный орган Министерства внутренних дел Российской Федерации.

Чтобы не оказаться жертвой мошенников, необходимо знать следующее:

- 1) сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок ее действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;
- 2) ни при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;
- 3) хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;
- 4) не сообщать пин-код третьим лицам;
- 5) остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;
- 6) лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;
- 7) внимательно читайте СМС-сообщения, приходящие от банка;
- 8) никогда и никому не сообщайте пароли и секретные коды, которые приходят вам в СМС-сообщении от банка;
- 9) помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС-сообщении от банка;
- 10) сотрудники банка никогда не попросят вас пройти к банкомату;
- 11) если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

12) не покупайте в интернет-магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

13) никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, мессенджерах, возможно мошенники взломали его аккаунт, сначала свяжитесь с этим человеком и узнайте, действительно ли он просит у вас деньги;

14) в информационно-телекоммуникационной сети «Интернет» не переходите по ссылкам на неизвестные сайты;

15) действуйте обдуманно, неторопливо.
