РОССИЙСКАЯ ФЕДЕРАЦИЯ
г. Иркутск

АДМИНИСТРАЦИЯ

КОМИТЕТ ПО СОЦИАЛЬНОЙ ПОЛИТИКЕ И КУЛЬТУРЕ

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ

664001, г.Иркутск, ул.Рабочего Штаба,9, www.admirk.ru тел. 52-01-71

от 23.10.2024 № 215-74-2440/24

на № _____ от _____

Руководителям муниципальных общеобразовательных организаций, расположенных на территории Куйбышевского района города Иркутска

Уважаемые руководители!

На основании письма прокуратуры Куйбышевского района города Иркутска от 17 октября 2024 года № 21-121-2024/3125-24-20250008 департамент образования комитета по социальной политике и культуре администрации города Иркутска направляет информационные памятки, направленные на противодействие преступности в сфере информационно-телекоммуникационных технологий (далее – памятки).

Необходимо обеспечить использование информации, указанной в памятках, в профилактической работе, а также разместить на официальном сайте и информационных стендах образовательной организации.

Приложение: на 3 л. в 1 экз.

Начальник департамента образования А.А. Головко

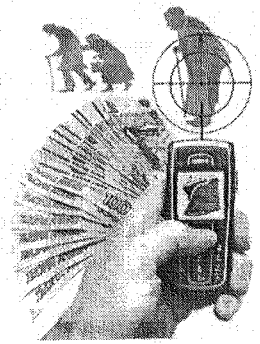
Исп.: Федорова В.Д.,
52-01-96

ПАМЯТКА

в целях предотвращения телефонного мошенничества

Иркутск
2024

В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от ребёнка до пенсионера, случаи телефонного мошенничества множатся с каждым годом. Как правило в организации телефонных махинаций участвуют несколько преступников, которые зачастую отбывают наказание в исправительных учреждениях. Мошенники разбираются в психологии, и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении. Чаще всего в сети телефонных мошенников попадаются пожилые люди или подростки, поскольку пожилые граждане зачастую испытывают чувство одиночества и изолированности, они доверчивы и легко поддаются внушению со стороны, а подростки доверчивы в силу того, что еще с детства не разучились мечтать и верить в лучшее.



Так что же такое телефонное мошенничество?

Телефонное мошенничество — вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомерное пользование ресурсами и услугами, хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, модификации информации или другого вмешательства в работу средств обработки или передачи данных информационно-телекоммуникационных сетей.

Наиболее распространенными видами телефонного мошенничества являются следующие:

1. Просьба о помощи

Поступает звонок с незнакомого номера, и мошенник, представившись родственником, знакомым или коллегой по работе, взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении какого-нибудь преступления: хранение оружия или наркотиков, нанесение телесных повреждений, хулиганство, участие в ДТП.

Далее в разговор вступает второй мошенник и представляется сотрудником правоохранительных органов. Он уверенным голосом сообщает, что совершено преступление и, если Вы хотите помочь, необходимо привезти определенную сумму в оговоренное место и передать какому-либо человеку или перевести на счет с помощью платежного терминала.

Либо абонент получает на мобильный телефон сообщение с незнакомого номера с просьбой положить на этот номер денежные средства, при этом добавляется, чтобы он не звони ие «мам

Возможен вариант, когда мошенник, представившийся работником правоохранительных органов, сообщает о возбуждении уголовного дела в Вашем отношении и требует деньги за «решение вопроса» о его прекращении.

В целях предотвращения преступных действий в этих случаях необходимо прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Также необходимо действовать и при получении сообщения о проблемах.

В разговоре с якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и уточнить информацию (например, действительно ли родственник или знакомый доставлен туда).

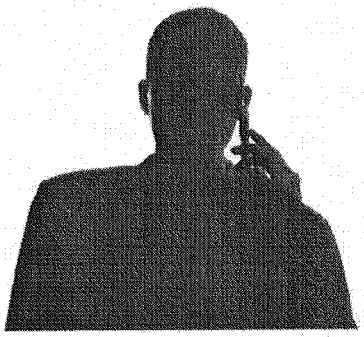
2. Мошенничество с банковскими картами

На телефон приходит сообщение о блокировке банковской карты и предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда абонент звонит по указанному телефону, мошенник сообщает, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просит сообщить номер карты и ПИН-код для ее перерегистрации.

Возможен вариант, когда преступник, представившись работником банка, сам звонит абоненту с целью получения ПИН-кода банковской карты.

С целью предотвращения преступных действий никому не сообщайте реквизиты банковской карты. Ни одна организация, включая банк, не вправе требовать ПИН-код. Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, там ответят, что никаких сбоев на сервере не происходило, а банковс киваться банком.



3. Звонок на платный телефонный номер

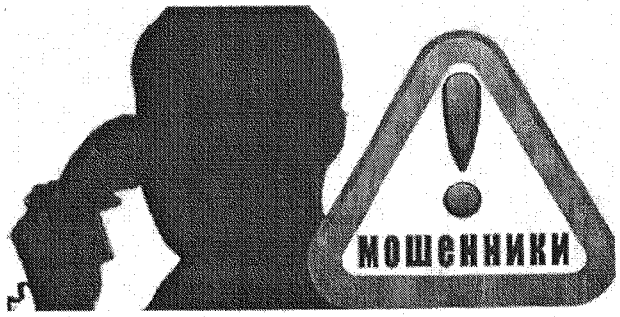
Абоненту приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с банковской картой и так далее. После того как абонент перезванивает, его долго держат на линии, и, когда он отключается, то оказывается, что с его счёта списаны крупные суммы.

С целью предотвращения преступных действий рекомендуется не звонить по незнакомым номерам, поскольку существуют сервисы с платным звонком (чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок). Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

4. Выигрыш приза

На мобильный телефон приходит смс-сообщение о выигранном призе либо поступает звонок с поздравлением в выигрыше в лотерее, акции и т.п. и необходимости связаться с «призовым» отделом. После того, как владелец телефона связывается с автором сообщения («призовым» отделом), его убеждают в честности акции и сообщают, что необходимо предварительно оплатить сопутствующую услугу или подоходный налог через систему денежных переводов.

Если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в



5. Акция оператора мобильной связи

Абонент получает сообщение об акции, проводимой его мобильным оператором. Например, предложение подключить новую эксклюзивную услугу, получить на какой-то период времени возможность осуществлять бесплатные звонки по стране и другие. Однако, для этого ему необходимо всего лишь отослать в службу информационной поддержки по сообщенным телефонам коды нескольких карт оплаты. Естественно, потом выясняется, что

оператор рекламных акций не проводил, а карты оплаты пополнили счета мошенников.

В целях предотвращения преступных действий необходимо перезвонить мобильному оператору для уточнения правил акции, новых тарифов и условий предоставления мобильной связи.

6. Ошибочный перевод средств

Абоненту приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок, что на счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. После перевода, такая же сумма списывается со счета абонента, так как мошенник, используя чек, выданный при переводе денег, обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер.

В целях предотвращения преступных действий не поддавайтесь на обман и попросите звонившего воспользоваться чеком для возврата ошибочно переведенных денежных средств.

7. Компенсация за лекарственные препараты

После заказа по почте средства для улучшения здоровья поступает звонок по телефону, в ходе которого неизвестный (например, представитель министерства здравоохранения, налоговый инспектор, сотрудник правоохранительных органов) сообщает, что приобретенный препарат якобы оказался подделкой и покупателю положена компенсация, но, чтобы получить эти деньги, необходимо заплатить подоходный налог с суммы и указывается номер счета, на который необходимо перевести деньги.

В целях предотвращения преступных действий необходимо прекратить телефонный разговор [illegible] организацию, предста[illegible] представился злоумыш[illegible] формации.

8. Телефонные вирусы

На телефон абонента приходит сообщение, для получения которого необходимо перейти по ссылке. При выполнении данной команды на телефон скачивается вирус и происходит постепенное списание с него денежных средств.

Также возможно, что при заказе какой-либо услуги через «якобы» мобильного оператора или при скачивании мобильного приложения абоненту приходит предупреждение: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции отправьте сообщение с цифрой 1, для отмены с цифрой 0». Если согласие получено, то с телефонного счета будут списаны деньги.

Мошенники используют специальные программы, позволяющие автоматически генерировать тысячи таких сообщений, следствием чего является списание средств с телефонов.

В целях предотвращения преступных действий не переходите по таким ссылкам и не звоните на номер, с которого отправлено сообщение.

Телефонное мошенничество не стоит на месте. Преступники постоянно придумывают новые способы отъема денег. В этой связи только бдительность поможет не стать жертвой злоумышленника.

Если же Вы стали жертвой телефонного мошенника следует незамедлительно обратит[illegible] ием.

телефоны ГУ МВД России по Иркутской области

02, ...