Способы защиты граждан от мошенничеств, совершаемых дистанционным способом

Как показывает практика, очень часто граждане, общаясь по телефону, а также в сети Интернет, с ранее неизвестными им лицами, добровольно переводят свои денежные средства в сумме до нескольких миллионов рублей мошенникам, которые действуя под различными предлогами звонят и настойчиво предлагают перевести денежные средства на «безопасные» счета для «защиты от мошенников», либо использовать денежные средства для совершения спекулятивных сделок на рынке криптовалюты с целью получения большой прибыли, и т.д.

В качестве способов защиты от такого рода мошенничеств следует рассматривать:

- незамедлительное прекращение общения с такими лицами, вне зависимости от того, кем они представляются – «сотрудниками банка», «сотрудниками полиции», «сотрудниками ФСБ», «сотрудниками Интернет-проекта» и т.д.;

- незамедлительное обращение в органы внутренних дел по телефонам 102, 112;

- блокирование номеров телефонов звонивших посторонних лиц на своем телефоне, смартфоне с целью предотвращения повторных звонков злоумышленников и поступления от них сообщений;

- при малейшем подозрении на перевод денежных средств с ваших счетов, незамедлительное блокирование банковских карт, счетов через приложение банка, а также путем обращения в банк лично или по телефону, указанному на сайте банка;

- при любом общении с посторонними лицами, кем бы они не представлялись, нельзя передавать им какие-либо сведения о себе, о своих счетах, пароли от входа в личный кабинет банка, в личный кабинет госуслуг, личный кабинет налогоплательщика, коды и пароли, поступающие вам в СМС, иных электронных сообщениях и т.д.;

- после окончания беседы всегда следует вспоминать какие данные вы сообщили постороннему о себе из вышеуказанных. Если это все-таки произошло, следует принять меры к незамедлительному блокированию ваших личных электронных кабинетов и обращению в полицию.

Следует проверять полномочия и личность звонящих вам путем звонка в правоохранительные органы, банки по телефонам, указанным на их официальных сайтах.

При наличии затруднений с дальнейшими действиями, в случае настойчивых звонков посторонних, рекомендуется, особенно для пожилых граждан, посоветоваться с ближайшими родственниками, сообщить им о возникновении такой проблемы.

ПОМНИТЕ: любое промедление с обращением в правоохранительные органы позволит мошенникам вывести Ваши денежные средства на другие счета и похитить их.

О наиболее распространенных способах кибер-мошенничества

Наиболее распространённые схемы телефонного мошенничества:

Обман по телефону: требование выкупа или взятки за освобождение, якобы, из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

Телефонный номер-«грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую, якобы, проводит радиостанция или оператор связи: вас просят приобрести карты экспресс-оплаты и сообщить коды, либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

Штрафные санкции и угроза отключения номера: якобы, за нарушение договора с оператором Вашей мобильной связи.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы, позволяющая получить доступ к SMS и звонкам другого человека.

Для общения с потенциальной жертвой *мошенники используют либо SMS, либо телефонный звонок.*

SMS – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – в надежде на доверчивого получателя.

Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом.

Цель мошенников – заставить Вас передать свои денежные средства «добровольно».

Для этого используются различные схемы мошенничества. Изъятие денежных средств может проходить разными способами. Вас попытаются заставить:

1)Передать деньги из рук в руки или оставить в условленном месте.

2)Приобрести карты экспресс-оплаты и сообщить мошеннику коды карты.

3)Перевести деньги на свой счёт и ввести специальный код.

4)Перевести деньги на указанный счёт.

5)Позвонить на специальный телефонный номер, который окажется платным, и с Вашего счёта будут списаны средства.

Есть несколько простых правил: отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых; не реагировать на SMS без подписи с незнакомых номеров; внимательно относиться к звонкам с незнакомых номеров.