Мероприятия по профилактике хищений денежных средств граждан, совершённых с использованием информационно-телекоммуникационных технологий

Сфера информационно-телекоммуникационных технологий (далее по тексту ИТТ) затрагивает все сферы жизни современного общества. Количество преступлений, совершаемых с использованием ИТТ, неуклонно растет, методы, способы и средства их совершения становятся все сложнее и изощреннее.

Так, в 2022 году подразделениями ОВД выявлено более 100 тыс. преступлений, совершенных с использованием ИТТ, в сфере компьютерной информации, с использованием сети «Интернет», а также с использованием средств мобильной связи.

Вопросы, связанные с использованием ИТТ на законодательном уровне регулируются Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Законодательные акты, разработанные на его основе, в целом позволяют Роскомнадзору во взаимодействии с операторами связи и организаторами распространения информации, осуществлять ведение «Единого реестра доменных имен, указателей страниц сайтов в ИТТ сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

Принятие Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств», позволил кредитно-финансовым организациям своевременно блокировать незаконные транзакции, возмещать ущерб от них.

В соответствии с Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс РФ», ужесточено наказание за хищение денежных средств с банковского счета или электронных денежных средств.

При этом имеющиеся нормативные правовые акты не в полной мере позволяют решать поставленные перед МВД России задачи.

Так, первичным способом борьбы с преступностью в сфере ИТТ является ее профилактика, которая берет свое начала с правил поведения граждан, в отношении которых происходят мошеннические действия в сфере ИТТ. Изучение видов преступной деятельности в сфере ИТТ, методов их совершения, методов достижения цели и обмана, изучение методик и правил поведения граждан при общении с преступниками, позволит профилактировать указанное направление преступной деятельности и пресечь наступление вредных последствий.

Наиболее распространенные виды мошенничеств в сфере ИТТ, а также признаки мошеннических схем:

1) приобретение товаров и услуг посредством сети «Интернет». Пример: создается сайт-«одностраничник», на котором выкладываются товары одного визуального признака. Цена за товары весьма привлекательная, ниже среднерыночной. При оформлении заказа Вам предлагают осуществить либо предоплату на карту банка или яндекс.кошелек, либо оплатить заказ «наложенным платежом». Присутствие возможности наложенного платежа обычно снижает бдительность. Однако, стоит помнить, что при получении посылки (товара) в отделении «Почта России» вы сначала оплачиваете наложенный платеж, который возврату на месте не подлежит, а уже после можете вскрыть упаковку посылки. Зачастую вместо оплаченного товара в посылке могут находиться предметы, которые не представляют ценности (доски, кирпичи и иные предметы), либо товары, стоимость которых низкая, относительно стоимости заказанного товара.

Признаки мошеннической схемы на сайтах: отсутствие отзывов покупателей, минимальный интерфейс, скудные контактные данные, переписка ведется с электронных почтовых ящиков.

Подобные мошеннические схемы могу осуществляться и посредством телефонных звонков с различных номеров, зачастую стационарных. Звонящий представляется сотрудником интернет - магазина, предлагает на выгодных условиях приобрести товар, а также говорит о том, что вы уже оформляли интернет-заказы и у вас скоплено определенное количество подарочных баллов, за счет которых Вам обеспечена скидка от стоимости.

2) Призыв о помощи. На интернет ресурсах злоумышленниками размещается ложная информация о наличии заболевания у беспомощного лица, и что необходимо дорогостоящее лечение. В связи с чем Вас просят оказать благотворительную помощь, путем перевода денежных средств на счета банковских карт, либо иными способами электронных платежей.

Конечно бывают жизненные ситуации, когда подобные призывы к благотворительности действительно могут помочь спасти жизнь кому-либо, однако, прежде чем принять подобное решение обратите внимание на следующее: размещены ли контактные данные родственников или родителей лица, которому нужна помощь, совпадают ли их данные с данными владельцев карт. Позвоните по указанным контактным номерам, а еще лучше попробуйте найти их в социальных сетях.

3) Звонок от родственника, попавшего в беду. Раздается звонок с неизвестного номера. Говорящий, адаптируясь по ситуации, здоровается, и говорит «это я». Жертва, сразу ассоциируя подсознательно говорящего с кем-то, которого она не узнала, пытается узнать и в итоге называет имя близкого человека. Злоумышленник, пользуясь ситуацией, соглашается с тем, что имя принадлежит ему, после чего, наладив психологический контакт с жертвой, начинает рассказывать историю о том, что он попал в беду (ДТП, попал в полицию за преступление, которое не совершал, и т.д.) При этом зачастую к разговору подключается его сообщник, представляясь каким-либо сотрудником госструктуры и подтверждает рассказанную историю. После чего «псевдородственник» просит перевести денежные средства, якобы для выхода из ситуации и его освобождения.

В сложившейся ситуации вы должны сразу помнить о том, что подобные виды мошенничеств существуют, и сразу же задать говорящему любой вопрос, связанный с вашим знакомством и т.п. Если говорящий пытается запутать вас и не может ответить конкретно, то сразу же прекратите разговор, дабы исключить психологическое воздействие на Вас.

4) Звонок от работника банка (представителя службы безопасности). Раздается звонок с незнакомого номера. Звонящий уверенным голосом представляется работником банка (в основном называется ПАО «Сбербанк»), уверенно утверждая, что жертва является клиентом банка, и что в отношении него происходят мошеннические действий, например, поступила заявка в банк на списание денежных средств. При этом говорящий задает неоднократно вопросы: производили ли вы переводы денежных средств, оплачивали ли вы товары через сеть интернет, снимали ли вы денежные средства с банковской карты в последнее время. Жертва, будучи введенной в заблуждение, начинает отвечать на вопросы. Наладив психологический контакт с жертвой, мошенник, под предлогом пресечения мошеннических действий и возврата якобы похищенных денежных средств, просит назвать номер карты жертвы, дату выпуска и CVC код, указанный на оборотной стороне карты. Обладая указанной информацией злоумышленник с легкостью, при помощи легитимно существующих систем электронных платежей, может беспрепятственно похитить со счета банковской карты денежные средства. Кроме того, иногда, при переводах с банковских карт на номер телефона жертвы приходят от банка смс-коды, подтверждающие переводы. Данные коды злоумышленник также пытается обманным путем выманить.

5) Звонок от сотрудника полиции (следственный комитет, прокуратура). Звонящий представляется сотрудником правоохранительных органов и т.д. после чего разъясняет информацию о том, что по паспорту потерпевшего в каком-либо субъекте РФ мошенники пытаются оформить кредит, при этом называют ложные ФИО с вопросом, знаком ли такое потерпевшему. При установлении контакта с потерпевшим, злоумышленники просят произвести различные манипуляции: оформить кредит в онлайн-кабинете и осуществить их перевод на номера телефонов и банковских карта, перевести личные сбережения на те же номера телефонов, назвать различные пароли, перейти по ссылкам и т.д.

Также мошенники могут звонит под личиной сотрудников правоохранительных органов и просить потерпевших поучаствовать в задержании мошенников, которые пытаются получить доступ в счетам потерпевших, для этого просят перевести все свои денежные средства на сторонний счет, якобы заморозив указанную сумму, обещая, что указанные денежные средства вернуться на счет потерпевших спустя какое-то время.

В указанной выше ситуации нужно помнить, что работники банка или сотрудники полиции не осуществляют подобных звонков. Даже если Вам позвонит работник банка, то он в праве только попросить Вас заблокировать вашу карту и обратится в ближайшее отделение банка. Данные банковской карты, такие как номер карты, а уж тем более код CVC передавать кому-либо запрещено, и никто не вправе у вас его требовать.

6) Приобретение товаров на сайтах объявлений (Авито и т.д.), заказ доставки чего-либо через сервисы «Блаблакар». Потерпевший сам инициирует заказ товаров или услуг, при этом при беседе со злоумышленником переходит для общения в иные сервисы, такие как «ВатсАп», «Телеграмм» и т.д. Уже в указанных сервисах злоумышленник либо просит перевести предоплату за товары и услуги, либо присылает ссылку якобы сервиса по переводу денежных средств, зачастую с логотипами «Авито оплата», после чего потерпевший переводит денежные средства, не получая при этом заказанные товары или услуги. Также имели место быть случаи, когда при вводе данных банковской карты потерпевшего в высланной ему ссылке, денежные средства начинали списываться автоматически в разных суммах, не запрашивая при этом какие-либо подтверждающие коды.

7) Звонок от банковской организации с роботизированным текстом. Потерпевшему раздается звонок с роботизированным текстом о том, что подана заявка в банк на перевод, либо на получение кредита на внушительную сумма. В этот момент не конкретизируется ни банк, в котором подана заявка, ни данные потерпевшего. После подобного звонка раздается звонок уже от якобы сотрудника банка, который уже дает потерпевшему указания, как выйти из ситуации, принуждая передать персональные данные, либо осуществить перевод денежных средств. В данной ситуации нужно помнить, что банковские работники могут звонить клиентам банка только с уведомительной информацией, никаких переводов в телефоном режиме осуществить не возможно. В случае получения подобного звонка стоит, при возникновении сомнения, обратиться в банк.

Особое внимание прошу уделить информации о возможных мошеннических действиях при помощи голосовых помощников в управлении банковскими счетами.

Если Вам звонят и просят ответить на вопросы фразами «да» или «нет», то есть вероятность того, что в это время происходит взлом вашего банковского счета при помощи голосового управления.