ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА МУРМАНСКОЙ ОБЛАСТИ
ПРОКУРАТУРА ГОРОДА АПАТИТЫ

Профилактика преступлений, совершаемых с использованием информационно-коммуникационных технологий

2023 ГОД

Профилактика преступлений, совершаемых с использованием информационно-коммуникационных технологий

Развитие современного общества, основанного на использовании огромного массива разнообразной информации, немыслимо без широкого внедрения компьютерной техники. Она служит для хранения и обработки информации, используется как средство связи и коммуникаций. За последние 4 года произошел резкий рост преступлений, совершенных с применением информационно-коммуникационных технологий или в сфере компьютерной информации – более, чем в 6 раз.

Более половины преступлений совершено с использованием сети «Интернет», значительное количество – с применением средств мобильной связи, расчетных (пластиковых) карт. К социальным причинам роста преступности в сфере ИКТ относится: - всеобщая компьютеризация, которая создает необходимую среду для деятельности компьютерных преступников; - противоречия между потребностями населения и возможностью их удовлетворения легальными способами в силу низкого уровня жизни; - легкомысленное отношение российского общества к компьютерной преступности; - доверчивость граждан при онлайн-покупке товаров и услуг (оплата до их получения, особенно через интернет-кошелек, а не через расчетный счет банка, помощь по объявлениям от благотворительных организаций через сайты-дублеры со сторонними реквизитами для перечисления денег). Профилактика особенно важна в отношении несовершеннолетних пользователей сети «Интернет». Учитывая, что значительную группу лиц, совершающих преступления в сети Интернет, составляют ранее не судимые учащиеся, в том числе и несовершеннолетние, с целью профилактического воздействия на них необходимо проводить профилактические мероприятия в школах, высших учебных заведениях, публиковать статьи на эту тему.

Анализ данных уголовно-правовой статистики свидетельствует о росте числа таких преступных деяний. Так, за 2020 год на территории Мурманской области с использованием информационно-телекоммуникационных технологий совершено более 4200 преступлений, что на 75% больше, чем в 2019 году. Из них 2189 – это мошенничества, совершенные, в том числе с использованием электронных средств платежа и в сфере компьютерной информации. Только за январь текущего года жертвами действующих дистанционно злоумышленников стали 308 жителей региона.

К наиболее типичным способам совершения преступлений с использованием информационно-телекоммуникационных технологий можно отнести следующие. Злоумышленники звонят гражданам, представляясь сотрудниками банков, называя их по имени, отчеству, просят сообщить

данные банковских карт (номер, CVC(CVV), PIN-коды и т.п.) для предотвращения якобы несанкционированного списания денежных средств либо оформления кредита. Используя эти сведения, получают удаленный доступ к личному кабинету клиента банка и переводят деньги без ведома собственника. При этом, преступники могут использовать программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка. Зачастую введенные в заблуждение граждане сами переводят денежные средства на счета, указанные мошенниками. Распространены хищения с использованием преступниками сервиса «Avito». Вводя гражданина в заблуждение относительно своего намерения приобрести или продать товар, в ходе телефонных разговоров злоумышленники узнают реквизиты банковской карты потерпевшего, при помощи которых списывают денежные средства со счета. В ряде случаев предлагается перейти по ссылкам для перевода денежных средств, после чего «продавец» не предоставляет оплаченный товар и не выходит на связь. Кроме этого, преступники массово рассылают SMS-сообщения следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру…». Большинство граждан, вместо того, чтобы сразу обратиться в свой банк для проверки поступившей информации, перезванивают по указанному в SMS-сообщении номеру и в ходе разговора передают злоумышленникам информацию о банковских реквизитах, после чего осуществляется незаконное списание денежных средств. Зачастую граждане сами переводят денежные средства на указанные преступниками «защищенные» счета якобы для их сохранения. Фактически денежные средства выбывают из законного владения, и собственник не имеет к ним доступа. Хищения денежных средств у граждан совершаются также путем направления SMS-сообщений о выигрыше, для получения которого необходимо перевести денежные средства на указанный абонентский номер. Распространены факты, когда преступники представляются родственниками либо знакомыми потерпевших, рассказывают, что попали в беседу (стали виновником дорожно-транспортного происшествия, задержаны сотрудниками полиции, срочно требуются деньги на операцию и т.п.) и просят предоставить им денежные средства. Злоумышленники взламывают электронную почту, аккаунты в социальных сетях, после чего от имени пользователя рассылают гражданам, сведения о которых имеются в контактах данного лица, просьбы о займе денежных средств. В результате деньги поступают на счет мошенника.

Чтобы не стать жертвой преступников, необходимо следовать определенным правилам:

1. Если получен звонок или сообщение в социальной сети с просьбой о срочной денежной помощи для знакомого или родственника, не стоит принимать решение сразу. Необходимо проверить полученную информацию, связавшись со своими родными и знакомыми.
2. Никогда и никому не сообщайте трёхзначный код на обратной стороне

Вашей банковской карты (CVV), это ключ к Вашим деньгам.
3. Нельзя сообщать никому личные сведения, данные банковских карт и СМС-пароли, которые могут быть использованы злоумышленниками для неправомерных действий.
4. Если по телефону Вас просят набрать комбинацию цифр в банкомате, прекратите разговор. Никогда не выполняйте действия с банкоматом «под диктовку» другого человека.

Необходимо помнить, что злоумышленники могут представиться сотрудниками банка, правоохранительного органа, учреждения здравоохранения и обращаться к Вам по имени и отчеству. Однако только мошенники будут просить сообщить реквизиты банковской карты, смс-пароль (код), CVV-код Вашей карты. В каждом таком случае необходимо завершить разговор. Сотрудники банка также не предлагают: - установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, для удаления вирусов с мобильного устройства); - перевести денежные средства на «защищенный счет»; - включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.

Мошенники постоянно придумывают новые уловки и способы обмануть нас, поэтому попытки защитить мобильные устройства уже стали частью нашей цифровой жизни. Тем не менее некоторые виды мошенничества опознать непросто, поэтому важно следить за появлением новых схем обмана и уметь их выявлять.

К наиболее распространенным видам дистанционного мошенничества, совершенного на территории Санкт-Петербурга и Ленинградской области, относятся:

«фишинг» — вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс — сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения. Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т,п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в

результате чего злоумышленники похищают принадлежащие им денежные средства.

«фарминг» — процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер и другие)

«двойная транзакция» (при оплате товаров и услуг продавец сообщает об ошибке и предлагает повторить операцию, а в дальнейшем денежные средства описываются дважды по каждой из проведенных операций)

Основные схемы телефонного мошенничества:

Обман по телефону.

Мошенник звонит с незнакомого номера и представляется родственником (знакомым) и взволнованным голосом сообщает, что задержан сотрудниками правоохранительных органов и обвиняется в совершении того или иного преступления (это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство). Далее в разговор вступает якобы сотрудник правоохранительных органов, который уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует перевести на определенный расчетный счет или передать какому-либо человеку. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам, но нередко человек, которому звонит мошенник, сам случайно подсказывает имя того, кому нужна помощь.

Аналогичным образом могут звонить мошенники сотрудникам государственных органов, либо предпринимателям и, представляясь, например, руководителем какого-либо государственного органа (правоохранительного, надзорного, контролирующего), под предлогом приезда комиссии проверяющих и требуют организовать либо «теплый прием» в форме бесплатного предоставления услуг (питание, подарки, организация отдыха и т. д.), либо перечислить определенную сумму денежных средств на указанный расчетный счет для организации досуга проверяющих или достижения необходимых положительных результатов проверки.

Как поступить в такой ситуации? Прервать разговор и перезвонить тому, о ком идет речь (либо в указанный государственный орган). Если телефон отключен, нужно связаться с его коллегами, друзьями и родственниками для уточнения информации.

SMS-просьба о помощи.

SMS-сообщения позволяют упростить схему обмана по телефону. Абонент получает на мобильный телефон сообщение: «У меня проблемы,

кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие. На сообщения с незнакомых номеров реагировать нельзя.

Телефонный номер-грабитель.

На телефон 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 Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь — и оказывается, что с Вашего счета списаны крупные суммы. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок. Единственный способ обезопасить себя от телефонных мошенников — не звонить по незнакомым номерам.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счет они снимаются с телефона. Не следует звонить по номеру, с которого отправлено SMS — вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

Выигрыш в лотерее или какого-либо приза.

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют это для своей деятельности и обмана людей. На Ваш мобильный телефон, как правило, в ночное время — приходит SMS- сообщения, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего, упоминаются известные иностранные модели , марки. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из вышеуказанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного денежную сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки и получения «кода регистрации». Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому, злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

Простой код от оператора связи.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

Как поступить в такой ситуации? Перезвонить своему мобильному оператору для уточнения условий, а также узнать, какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

Ошибочный перевод средств.

Абоненту поступает SMS — сообщение о поступлении средств на его счет с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности, деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа.

Как поступить в такой ситуации? Если Вас просят перевести, якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

Мошенничества с банковскими картами

Банковская карта — это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Вам приходит сообщение о том, что Ваша банковская карта заблокирована.

Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, то Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. Злоумышленникам нужен лишь номер Вашей карты и ПИН-код, как только Вы их сообщите, деньги будут сняты с Вашего счета. Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу

поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банкоматом.

Если Вы утратили карту немедленно ее блокируйте.

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной.

Совершая операции пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой.

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону».

Если банкомат долгое время находится в режиме ожидания или самопроизвольно перезагружается -откажитесь , от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Для проведения оплаты бесконтактной картой рекомендуется просто приложить её к терминалу. Ввод ПИН-кода не требуется, если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено. Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумме или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

Как обезопасить себя от мошенников:

1. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.
2. Не устанавливать и не сохранять без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).
3. Использовать пароли не связанные с Вашими персональными данными.
4. Не сообщать данные карты, пароли и другую персональную информацию.
5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

6. По всем возникающим вопросам обращайтесь в выдавший карту банк.

7. Не выполняйте никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.

8. Не переходите по ссылкам, которые приходят по e-mail, либо SMS.

9. Обращайте внимание на все сообщения от банка (например, если они содержат грамматические ошибки).

10. Не перезванивайте по номерам, которые приходят на e-mail либо по SMS.

Если Вы стали жертвой преступника, необходимо незамедлительно обратиться в органы внутренних дел с соответствующим заявлением лично либо позвонить по телефонам 102 или 112. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Также следует принять меры к блокировке банковской карты.