Прокуратура РС (Я): Граждане, будьте бдительны, не попадайтесь на уловки мошенников!

Последнее 10-летие информационные технологии прочно вошли в жизнь практически каждого человека. Однако, с безграничной пользой, которую предоставляют мобильные Интернет услуги в нашу жизнь, к сожалению, входят и преступные посягательства. По данным информационного центра МВД Республики Саха (Якутия) за 12 месяцев 2020 года зарегистрировано 2287 преступлений, совершенных с использованием информационно телекоммуникационных технологий (2019 - 1583), рост по сравнению с предыдущим годом составил 44,5%. За 3 месяца с начала т.г. зарегистрировано уже 778 преступлений рассматриваемой категории (2019 - 472), рост составил 64,8%.

Почему важно это знать?

Мобильные и интернет мошенничества в подавляющем большинстве случаев совершаются гражданами, находящимися за пределами территории республики и даже страны. Преступления, совершенные неустановленными лицами из других регионов, использующими IP-телефонию или телефонные номера в виду технических сложностей – остаются не раскрытыми. Потому что, обычно мошенники номера телефонов или несколько платежных систем регистрируют на третьих лиц, которым пользуются только перед тем, как обналичить похищенные денежные средства.

Какие виды преступлений угрожает?

Большую часть преступлений составляют мошенничества, связанные с использованием мобильных средств связи и сети Интернет (ст. 159 УК РФ). В 2020 году через Интернет гражданам и организациям причинён ущерб на сумму почти 132 млн. рублей. За это время количество преступлений увеличилось на 64,5% %. (2020 - 1 907, 2019 - 1159).

Другую значительную часть преступлений в сфере ИКТ составляют так называемые «дистанционные хищения» или кражи, связанные с неправомерным списанием денежных средств с банковских карт граждан (ст. 158 УК РФ - кража). Таких преступлений в 2020 было - 754. Причинён ущерб на сумму почти 52 млн. рублей.

Кроме того, данную категорию преступлений составляет незаконных сбыт наркотических средств (ст. ст. 228, 228.1 УК РФ) - 522 (561) и преступления в сфере компьютерной информации (ст.ст. 272-274 УК РФ) – 29 (14), т.е. рост в 2 раза.

Кто становиться жертвами этих преступлений?

Является большим заблуждением считать, что на уловки мошенников попадаются только пожилые граждане, молодёжь и «недалёкие» граждане. Жертвами, как правило, становятся работающие граждане трудоспособного возраста от 25 до 55 лет (42,5 %), имеющие постоянный источник дохода. На пожилых граждан и молодёжь приходится всего 13-14 % пострадавших. Жертвами названных преступлений становятся граждане, обладающие денежными средствами на банковских счетах либо проявляющие заинтересованность в приобретении товаров, либо услуг через Интернет. Наибольшее количество пострадавших

отмечено в г. Якутске, Мирном, Нерюнгри, Удачном, а также в Алданском, Ленском, Мегино-Кангаласском, Вилюйском и Чурапчинском районах. Это не означает, что данные преступления не коснуться граждан, проживающих в других районах.

Какие виды мошенничества существуют?

По данным полиции, в настоящее время на территории республики преобладают 3 наиболее распространённых способа совершения дистанционных хищений:

- мошенники совершают хищения посредством использования подложных объявлений на интернет-площадках (Авито, Дром, Юла и т.д.) о купле-продаже или аренде различного имущества;

- мошенники представляются работниками банковских организаций, полиции или других представителей власти или организаций;

- создание злоумышленниками ложных интернет-сайтов, похожих на сайты известных банков, магазинов, которые пользуются у пользователей популярностью и доверием. Через ложные сайты происходит хищение реквизитов платежных карт;

- распространение злоумышленниками в сети Интернет и социальных сетях предложений заработать на процентах на так называемых «биржах», «инвестиционных компаниях», получить быстрый заработок.

Это не означает, что нет и не будет других видов. Мошенники ежедневно изобретают новые способы, виды, играя на слабостях людей. А именно на беспокойстве о здоровье, страхе за близких, страхе потерять свои деньги, и желании купить что-то дешевле. Также на заманчивых и интересных предложениях, денежной выгоде, потребности в заработке, информации для улучшения своей жизни и даже на желании поймать и наказать мошенника.

Как совершается интернет-мошенничество?

Мошенники совершают хищения посредством использования подложных объявлений о купле-продаже или аренде различного имущества на таких площадках, как Авито, Дром, Юла и т.д. Это могут быть объявления, как о продаже, так и о покупке имущества. В ходе общения под любым, в том числе «объективным» предлогом, мошенники могут предложить сообщить данные вашей банковской карты или предлагают перечислить аванс за бронирование, залога и т.д. Продавец по объявлению может попросить аванс за приобретаемую вещь, либо реквизиты вашей карты для перечисления аванса или залога вам, после чего перестает выходить на связь.

Поэтому следует знать, что приобретение товаров, в том числе авиабилетов, услуг посредством сети Интернет, не важно в интернет-магазине или с рук – это большой риск.

Интернет-сайт магазина может оказаться поддельным, а продавец или покупатель могут быть аферистами. Важно всегда помнить, что мошенники работают ежедневно, вне зависимости от времени суток.

Как не стать жертвой интернет-мошенничества?

Нельзя перечислять деньги авансом, но и наложенный платёж, к сожалению, не гарантирует то, что вы получите товар, на который вы рассчитывали. Вместо него вы можете получить так называемую «куклу» или совсем ничего. Всегда следует лично проверять исправность и наличие в предмете покупки обещанных свойств и возможностей. Рассчитываться только по факту получения.

Поэтому либо приобретайте товары в простом магазине, либо пользуйтесь только проверенными интернет-магазинами, либо сервисами, у которых в вашем городе есть офисы. Причём надо точно знать интернет-адреса этих магазинов, чтобы не попасть на поддельный сайт. Не делайте покупок со своих зарплатных карт, заведите для покупок специальную карту, например, с cashback или travel бонусами, и переводите на неё ровно столько денег, сколько необходимо на покупку.

Авиа и железнодорожные билеты приобретайте в авиакассах или исключительно на проверенном сайте авиакомпании (его адрес можно уточнить по телефону в авиакомпании). Кстати, многие не знают, что при покупке авиабилета cashback на банковскую карту начисляется только в том случае, если вы рассчитываетесь непосредственно банковской картой. Поэтому не стоит приобретать авиа и ж/д билеты в Интернете.

А как крадут деньги с банковской карты?

Основными способами (механизмами) хищений денежных средств с банковских карт являются:

- звонки или рассылка сообщений злоумышленниками, которые представляются работниками банка или государственными служащими.

Потерпевшие под воздействием обмана сами передают злоумышленникам персональные данные, одноразовые пароли для входа в приложения (например, Сбербанк-онлайн).

В результате чего появляется возможность снятия денежных средств с банковской карты потерпевших;

- совершение покупок похищенной или найденной банковской картой в торговых организациях. Очень часто мошенники представляются работниками банковских организаций, полиции или других органов, организаций, якобы, выполняют возложенные на них функции. Так, например, гражданам поступают звонки с такой информацией: «Вам звонят со службы безопасности банка, зарегистрирована попытка несанкционированного списания средств с вашей банковской карты». Для отмены или блокировки операции вам предлагают продиктовать реквизиты банковской карты или назвать код, поступивший по СМС, либо предлагают совершить какую-то операцию в банкомате.

Также могут говорить: «Взломан ваш личный кабинет мобильного оператора и поэтому вы не получаете СМС-уведомления банка об операциях, совершаемых по вашей банковской карте. Вам необходимо назвать код снятия переадресации СМС».

Злоумышленники делают повторные звонки даже тем клиентам, которые уже ранее пострадали от действий телефонных мошенников. Они представляются сотрудниками полиции и предлагают оказать содействие в возврате средств или поимке преступника. Так, есть случаи, когда по просьбе звонившего, якобы, сотрудника «полиции» граждане даже шли в банк «ловить мошенника». Одна московская блогерша «повелась» на такой звонок с предложением поймать недавно действительно звонившего ей мошенника. В процессе такой липовой спецоперации потеряла более 1 млн. рублей.

Также, по-прежнему могут быть и давно известные всем сообщения о том, что «ваш близкий задержан полицией или попал в беду и нужно срочно заплатить, чтобы спасти».

Кроме этого могут сообщить о начислении денег по ошибке и попросят вернуть средства на другой реквизит. Деньги по ошибке действительно могут поступить от такого же обманутого человека, но вот попросит вернуть их обратно уже мошенник.

Все способы мошенничества не перечислить – их достаточно много, и они постоянно меняются. Так, например, в последнее время получили распространение случаи, когда под видом сообщения с портала Госуслуг могут прислать электронное письмо с предложением ввести страховой номер СНИЛС для дальнейшего получения положенных социальных выплат, а также данные банковской карты, на которую должны поступить деньги. Звонки и сообщения могут прийти с известного всем номера Сбербанка 900.

Как не потерять деньги с банковской карты?

Первое, что надо усвоить, чтобы не стать потерпевшим от мобильного мошенничества, это не надо доверять звонящим вам на сотовый телефон неизвестным гражданам, хоть сотрудник банка, полиции, службы судебных приставов и т.д. Нельзя совершать какие-либо действия с банковской картой ни в онлайн-банке, ни в банкомате по просьбам звонящих вам неизвестных людей.

Не надо ходить на назначенные вам встречи вне официальных кабинетов банка, полиции и т.д. Найдите сами телефон банка, полиции, судебных приставов и позвоните и выясните имеется ли та проблема, о которой вам сообщили.

Только не надо при этом спрашивать номер телефона у самого звонящего вам неизвестного лица. Кроме этого, в соответствии со ст. 210 Гражданского кодекса РФ гражданин несёт бремя содержания своего имущества, а, следовательно, должен обеспечивать сохранность своего имущества, следовательно, не допускается разглашение данных банковской карты.

Граждане должны знать, что обеспечение конфиденциальности данных банковской карты, а именно пин-код, срок действия и CVC-кода, а также код СМС оповещения, подтверждающих совершение банковских операций, является их гражданской обязанностью и не допускается разглашение данных сведений посторонним лицам.

Ни при каких обстоятельствах нельзя сообщать никому пин, CVC-коды и срок действия банковской карты, а также коды из СМС оповещения. Это конфиденциальные данные вашей банковской карты.

Кроме того, мошенничество всегда есть там, где предлагают быстрый заработок — на биржевых площадках для инвестирования. Давно известно, что бесплатный или «супер выгодный» сыр бывает только в мышеловке. Любые активно рекламируемые в Интернете предложения произвести выгодное вложение — мошенничество или финансовая пирамида. Мошенники могут выступать и от имени известных биржевых площадок и вносить предложения, очень похожие на достоверные.

Хотите безопасно инвестировать средства – идите в банк, заключайте договор инвестиционного счета.

Можно ли распознать мошенника по голосу?

Вы никогда не распознаете мошенника по голосу. Он всегда в разговоре с вами будет вести себя очень непосредственно, очень квалифицированно, грамотно и предельно корректно, внушая доверие.

Внимание! Разъясните вашим близким, не имеющим работы, что нельзя «вестись» на предложения работы сомнительного характера с высоким заработком. Они могут стать соучастником преступления в сфере оборота наркотических средств. Гражданам, ищущим работу, следует знать, что они могут наткнуться на объявления, в которых открыто или завуалированно предлагают работу по закладке тайников с наркотиками. Если человек соглашается на такую работу, он становиться соучастником преступления по сбыту наркотических средств. Наказания по этой категории преступлений назначаются, как за особо тяжкие преступления. Можно лишиться свободы на более 10 лет. А за сбыт наркотиков в особо крупных размерах можно получить 20 лет колонии и даже пожизненное заключение.

Среди граждан, которые поддаются соблазну на такую работу бытует мнение, что эта преступность является теневой. Между тем, правоохранительным органам давно известны все схемы распространения. Граждан, взявшихся за такую работу, отслеживают и задерживают.

Поэтому, вместо того, чтобы поддаться таким «приглашениям», «уговорам» лучше выполнить свой гражданский долг и сообщить о таких «работодателях» в правоохранительные органы.

Чтобы найти легальный заработок лучше обратиться на биржу труда, где можно не только получить пособие по безработице и рассмотреть вакансии, но и пройти профессиональное переобучение. Следует помнить, что одной из форм занятости является самозанятость и предпринимательская деятельность А мнение людей о том, что у них нет предпринимательских способностей в подавляющем большинстве случаев – ошибочно. Обучение «Основам предпринимательской деятельности» бесплатно можно пройти в Центре занятости или в центрах «Мой бизнес», где также расскажут, как начать предпринимательскую работу, какие есть неохваченные ниши в бизнесе, льготы и гарантии (гранты и микрозаймы, поручительства в банках) у начинающих предпринимателей и малого бизнеса.

Доведите данную информацию до сведения Ваших близких, защитите их! Будьте бдительны! Не попадайтесь на уловки мошенников!