ОБРАЩЕНИЕ
к населению Республики Саха (Якутия)

Дорогие граждане, будьте бдительны! Не попадайтесь на уловки мошенников!

Причина нашего обращения к Вам?

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, зарегистрированные на третьих лиц, пользующимися перед обналичиванием похищенных денежных средств, несколькими платёжными системами, в виду технических сложностей – **остаются не раскрытыми!**

Какие виды преступлений с использованием ИКТ Вам угрожают?

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

Другую значительную часть преступлений в сфере ИКТ составляют т.н. «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 пенсионеры, 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 посредством сети Интернет.

Наибольшее количество пострадавших проживало в городах Якутск, Мирный, Нерюнгри, Удачный, а также Алданском, Ленском, Мегино-Кангаласском, Вилюйском и Чурапчинском районах. Но это не означает, что данные преступления не коснуться граждан, проживающих в других районах. Коснуться!

Какие виды мошенничества Вам угрожают?

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 органов или организаций;
- создание злоумышленниками ложных интернет сайтов, похожих на сайты известных банков, интернет-магазинов, которые пользуются у пользователей доверием, через которые 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.

Но это не означает, что нет и не будет других видов. Мошенники ежедневно изобретают новые способы, играя на слабостях людей, а именно на здоровье, страхе за близких, страхе потерять свои деньги, желании купить подешевле, заманчивых и интересных предложениях, денежной выгоде, потребность 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 интернет-площадках Авито, Дром, Юла и т.д., причём это могут быть объявления, как о продаже, так и о покупке имущества, в ходе общения под любыми, в т.ч. «объективными» предлогами вам предлагают сообщить данные вашей банковской карты или предлагаю перечислить аванс под предлогом бронирования, залога и т.д.

Продавец по объявлению может попросить аванс за приобретаемую по объявлению вещь, либо реквизиты вашей карты для перечисления аванса или залога вам, после чего перестанет выходить на связь.

Поэтому следует знать, что приобретение товаров, в т.ч. авиабилетов, либо услуг посредством сети Интернет, не важно в интернет-магазине или с рук у граждан – это большой риск!

Интернет-сайт магазина может оказаться поддельным, а в качестве физического лица – как продавца, так и покупателя – может выступить аферист!

Важно всегда помнить, что мошенники орудуют ежедневно, в любое время суток.

Как не стать жертвой интернет-мошенничества?

Нельзя перечислять деньги авансом, да и наложный платёж, к сожалению, не гарантирует, что вы получите именно тот товар, на который вы рассчитывали. Вместо него вы можете получить т.н. «куклу» или совсем ничего. Следует лично проверять исправность и наличие в предмете покупки обещанных свойств и возможностей и 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, т.к. wildberries, Почта России, aliexpress, 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 говоря, многие не знают, что при покупке авиабилета cashback на банковскую карту начисляется только в том случае, если вы рассчитываетесь непосредственно банковской картой, а не в интернете. 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 граждан 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 в торговых организациях, с помощью ранее похищенной или найденной банковской карты.

Очень часто мошенники представляются работниками банковских организаций, полиции или других органов или организаций и якобы выполняют возложенные на них функции.

Так, например, гражданам поступают звонки такого характера, как:

- «вам звонят со службы безопасности банка, зарегистрирована попытка несанкционированного списания средств с вашей банковской кары, 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;

- «взломан ваш личный кабине 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, имеются случаи, когда по просьбе звонившего якобы сотрудника полиции» граждане даже шли в банк «ловить мошенника»! Одна московская блогерша «повелась» на звонок т.н. «сотрудника полиции» с предложением поймать недавно действительно звонившего ей мошенника и 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 заплатить сотруднику полиции или врачу, чтобы спасти».

Вам могут сообщить о начислении денег по ошибке и попросят вернуть средства по другим реквизитам. Деньги по ошибке действительно могут поступить от такого же обманутого человека, но вот попросит вернуть их уже мошенник.

Все способы мошенничества не перечислить, их масса и они постоянно меняются!

Так, например, 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 могу прийти даже с известного всем номера Сбербанка 900.

Как не потерять деньги с банковской карты?

Первое, что надо усвоить, чтобы не стать потерпевшим от мобильного мошенничества – наша материальная безопасность в наших руках!

Не надо доверять звонящим вам на сотовый неизвестным гражданам, будь то сотрудник банка, полиции, службы судебных приставов и т.д. Нельзя совершать какие-либо действия с банковской картой, в том числе в банкомате по просьбам и предложениям звонящих вам неизвестных лиц, в т.ч. «банковских работников». Не надо ходить на назначенные вам встречи вне официальных кабинетов банка, полиции и т.д. Найдите сами телефон банка, полиции, судебных приставов и т.д., перезвоните туда 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 того, в соответствии со ст. 210 Гражданского кодекса РФ гражданин несёт бремя содержания своего имущества, а, следовательно, должен обеспечивать сохранность своего имущества, в т.ч. находящегося на банковской карте, а следовательно, не допускается разглашение данных банковской карты.

В указанной связи, что касается банковских карт, то граждане должны знать, что обеспечение конфиденциальности данных их банковской карты, а именно пин-кода, срока действия и CVC-кода, а также кодов СМС оповещения, подтверждающих совершение банковских операций, является их гражданской обязанностью и не допускать разглашение данных сведений посторонним лицам!!!

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

Кроме того, мошенничество всегда есть там, где предлагают быстрый заработок, в т.ч. на **биржевых площадках для инвестирования**. Давно известно, что бесплатный или «супер выгодный» сыр бывает только в мышеловке. Любые активно рекламируемые в Интернет 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 известный 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 Вам 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!

Всем 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 - более 10 лет лишения свободы. А за сбыт наркотиков в особо крупных размерах можно получить 20 лет колонии и даже пожизненное лишение свободы.

У 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 на искушение такой работы, лучше выполнить свой гражданский долг и сообщить о таких «работодателях» в правоохранительные органы.

А 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 деятельность, какие есть неохваченные ниши в бизнесе, льготы и гарантии (гранты и микрозаймы, поручительства в банках) у начинающих предпринимателей и малого бизнеса. А залогом успеха является постановка цели и движение к ней!

Доведите данную информацию до сведения Ваших близких, защитите их!

Прокуратура Республики Саха (Якутия)

Ежегодно увеличивается число обманутых владельцев банковских карт. Оружием мошенников стал телефон. Как обезопасить себя и сохранить свои деньги?

По данным РБК за 2019 год почти каждый десятый россиянин (около 9%) терял значительную для себя сумму денег из-за телефонного мошенничества, а каждый третий (33%) признался, что он или его близкие сталкивались с таким мошенничеством. Только 4% опрошенных обращались в правоохранительные органы.

Также по данным за 2018 год объем несанкционированных операций по картам вырос на 44% и составил 1,4 млрд рублей. В законе «О национальной платёжной системе» говорится, что если деньги с карты списаны без согласия клиента, то банк должен вернуть похищенную сумму. Однако таких случаев ещё не было. Банки не возвращают средства, потому что не могут различить действия клиентов и мошенничество: для этого суд должен установить виновных, а полиция не в состоянии их найти.

Знайте способы обмана!

Звонок из банка. Сейчас этот способ самый частый. В основном обзванивают клиентов крупных банков — в них обслуживается очень много людей. Из 50–100 звонков из таких «колл-центров» хотя бы один срабатывает. Клиенту звонят с использованием программ для подмены номера либо с номера, который раньше действительно принадлежал банку. Они представляются сотрудниками финансовой организации и выманивают пароли или коды для входа в личный кабинет или подтверждения перевода денег.

Звонок от родственника. Звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции. Причина — ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство. Мошенник просит перевести деньги на определенную карту — по легенде это карта друга или «помощника».

Звонок–грабитель. Человек поднимает трубку. Его приветствуют фанфары и довольный голос. Разговор тянется долго, а после выясняется, что он был платным. Есть и другая вариация такого звонка. Мошенники делают короткий звонок, чтобы он отразился на экране телефона как пропущенный. Когда человек перезванивает, со счета списывается фиксированная сумма.

Подозрительные смски. На телефон приходит сообщение от банка или оператора связи. В нем — просьба отправить определенный код или перейти по ссылке. Часто мошенники регистрируют адреса, похожие на названия известных организаций. Разница будет в одной букве — это получается заметить не сразу.

Как действуют мошенники?

Чаще всего те, кто снимает деньги у доверчивых граждан, — не один и не два человека. В «теневом» интернете есть много площадок, предлагающих продажу информации. Среди баз данных есть и банковские. Другими словами, весь ваш профиль в банке мгновенно доступен любому человеку, способному немного заплатить. Можно считать это нарушением Федерального закона №152-ФЗ. Фактически доказать это нарушение маловероятно.

Подделка номеров тоже теневая услуга. Имея доступ к системе небольшого мобильного оператора, можно подменить номер. В итоге преступник звонит со своего номера, а у абонента высвечивается любой другой, в том числе телефон банка. Как правило такие звонки могут предлагать зарубежные компании.

За день маленькая группа из нескольких человек вполне может зарабатывать несколько миллионов рублей.

Признаки мошенничества!

1. **При долгом общении собеседник начинает нервничать.** Если вы все же взяли трубку, то не ведитесь на рассказы мошенника о тестированиях новых систем или невозможности видеть ваши операции по карте. Так он пытается вытянуть ваши данные. Можно потянуть время и заставить злоумышленника нервничать — сказать, что ищете карту и «висеть» на телефоне минут 10-15. Или завершите разговор фразой «да, это я снимал деньги, все в порядке!». Если преступник понимает, что жертва что-то заподозрила, он просто прекратит разговор и продолжит обзванивать других. Не давайте повода усыпить свою бдительность.

Пример из жизни:

«Где-то полтора года назад я продавал бенгальских котят. Позвонила женщина — представилась руководителем какой-то компании. Якобы она решила купить котенка для своей племянницы, сама живет не в моем городе, поэтому сделку надо было провести с переводом денег.

Очень убедительно рассказала о себе, компании. Например, что котенка заберут их курьеры — «они как раз проезжают N, заедут, заберут и отдадут вторую часть денег». Задавала правильные вопросы о котятах.

Когда сошлись на цене, предложила перевести мне половину денег на карту. И сказала, что со мной свяжется человек из их финотдела. Затем перезванивает молодой человек. Представляется то ли юристом, то ли экономистом из их компании. Объясняет, что для перевода денег ему нужен номер карты, номер счета, дата, фио и код с обратной стороны карты. Такие условия необходимы, потому что «деньги переводят со счета компании, поэтому физлицо должно предоставить все эти данные, чтобы всё легально провести через бухгалтерию».

2. **Смс «от банка» перешло в новую переписку.** В таком сообщении может быть ссылка «для смены тарифа» или «для подтверждения зачисления средств». В таких сообщениях можно заметить ошибки в словах. Могут быть ошибки и в «имени» отправителя. Если нашли, то не сомневайтесь — это мошенники. Не переходите по ссылке, а сообщение удалите.

3. **Собеседник спрашивает данные карты или смс-код.** Смс-код приравнивается к паролю и по сути является простой электронной подписью.

Сотрудники банка никогда его не спросят, а номер карты они и так знают. Кроме того, подозрительный собеседник начнет придумывать новые способы получить ваши данные. Если в процессе разговора вам приходят «смс от банка» не сообщайте информацию из них и не переходите по ссылкам.

Пример из жизни:

«— Здравствуйте, ВВ! Вас беспокоит служба безопасности «Хорошегобанка». Меня зовут Усачев Дмитрий Сергеевич, я младший специалист. Мы тут зафиксировали подозрительную активность по вашей карте. Несколько минут назад пытались перевести 3 624 рубля. Это вы были?

— Да, это я снимала деньги.

— Хорошо, тогда скажите, сколько на ваше имя карт оформлено? Какая последняя операция была по ним — перевод, снятие, оплата?

— Это ж вы и сами можете посмотреть.

— У нас новая система безопасности, и этого всего не видно.

— Тогда мне тоже этого не видно.

— То есть, вы отказываетесь от проведения проверки? Подтвердите свой отказ устно в полной форме.

— До свидания!».

Как защитить свои деньги?

По данным опроса «Лаборатории Касперского», каждый пятый россиянин (21%) никак не защищает свой телефон от подозрительных звонков. Половина респондентов (51%) ответили, что не берут трубку, если видят на экране неизвестный номер. Еще 17% россиян используют специализированное ПО для защиты от спама и мошенничества, а 37% — встроенные возможности телефона, например черные списки.

Простые способы обезопасить себя и свои деньги:

1. Не принимайте звонки со скрытых или неизвестных номеров. Можно установить на телефон приложение, которое ищет владельца номера в интернете. Например, сервис Яндекса помогает избежать подозрительных звонков и спама. Нежелательные номера заносите в «чёрный список». Если вы поменяли номер своего телефона, предупредите об этом родственников и друзей.

2. Не сообщайте никому данные своей карты. Не сообщайте коды из смс. Если забыли карточку в общественном месте — заблокируйте.

3. Не принимайте звонки с подозрительных номеров. Не перезванивайте по ним. Ни спрашивайте у них телефон банка, по которому могут что-либо подтвердить, ищите его на своей банковской карте.

4. Держите связь с родственниками и друзьями. Если вам звонят с просьбами о помощи, сбросьте звонок. Перезвоните «жертве».

5. Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.

6. Не указывайте настоящий номер телефона и не расплачиваться основной картой на малоизвестных сайтах.

7. Не паникуйте, если вам пишут о блокировке счета. Позвоните в банк по номеру на сайте или на карте.

Прокуратура Республики Саха (Якутия)
677000, г. Якутск, пр. Ленина, 48,
http://https://epp.genproc.gov.ru/web/proc_14

Прокуратура Республики Саха (Якутия)

Телефонное мошенничество. Как распознать и защититься?

Якутск, 2020 год