Мошенничество в Интернете

Наиболее распространённые ситуации мошенничества с использованием Интернета:

- Хищения под видом продажи товара с использованием торговых интернет-площадок;

- Обман покупателей при покупке в лже-интернет магазинах;

- Создание интернет-сайтов "двойников" различных банков, а также по продаже товаров.

Хищения денежных средств с банковских счетов физических лиц с использованием неправомерного доступа к банковским картам потерпевших посредством сотовой связи и Интернета:

а) Получение сведений о персональных данных и банковских картах граждан посредством фишинговых сайтов и вредоносных программ с целью оплаты различных услуг и товаров, а также перевода денежных средств;

б) Интернет-мошенничества с использованием мобильных средств связи - получение под различными предлогами данных банковской карты и секретного кода, расположенного на обратной стороне карты с целью возможности хищения денежных средств.

ЗАПОМНИТЕ!

- Не производите предоплату какого-либо товара.

- Деньги отдавайте только в случае, если заказанный Вами товар проверен и полностью устраивает.

- При входе на сайты известных Вам банков, организаций или торговых площадок **внимательно изучите** открывшуюся страницу на экране (отличия от настоящего сайта, как правило, незначительны. Открытый Вами сайт может оказаться "двойником"!).

- Ни под каким предлогом и ни при каких обстоятельствах не сообщайте незнакомым лицам цифры, указанные на банковской карте.

Профилактика мошеннических действий в сети Интернет

Покупки через Интернет – это без сомнения очень удобно. Сфера Интернет-услуг расширяется, доходы сетевых ритейлеров растут, а люди все чаще предпочитают заказ товаров в сети походам по магазинам. Однако удобство Интернет-технологий распространяется не только на продавцов и покупателей. Мошенники также по достоинству оценили новые формы торговли и активно используют их своих целях.

Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег мы рекомендуем вам обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов.

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

На что следует обратить внимание? Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.

На что следует обратить внимание? Создание Интернет-магазина – дело нескольких часов, изменение его названия и переезд на другой адрес – дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

На что следует обратить внимание? Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия.

На что следует обратить внимание? Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы сделки. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие.

На что следует обратить внимание? Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

ВЫВОД

Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки. Если под их описание подходят два или более признака, мы настоятельно рекомендуем вам воздержаться от контактов с данным продавцом или магазином.

Как избежать потенциально опасных сделок, совершая онлайн-покупки или продажи в Интернете

Интернет-технологии все больше и больше позволяют активным пользователям Интернета расширять свои возможности. Не выходя из дома, вы свободно можете осуществлять общение, приобрести нужные или продать ненужные вам вещи, невзирая на время и географию. Однако такое удобство привлекает не только продавцов или покупателей, но и мошенников.

Для того чтобы радость онлайн-покупок не была омрачена потерей денег мы рекомендуем вам обратить внимание на некоторые признаки потенциально опасных сделок.

1. Лже-покупатель якобы заинтересовался выставленной вами на продажу вещи. Под видом осуществления оплаты он просит у вас реквизиты вашего банковского счета и цифры, пришедшие в смс-сообщении на ваш телефон. При овладении данной информацией мошенник тут же входит в ваш личный кабинет банка, клиентом которого вы являетесь, откуда списывает все имеющиеся на счетах деньги.

Так полицию с заявлением о краже неизвестным с банковского счета денег в сумме 470 000 рублей обратилась 41-летняя женщина.Она сообщила, что ей позвонил неизвестный гражданин и под предлогом покупки картины, которую она продавала по объявлению на одном из сайтов, попросил продиктовать номер карты. После разговора с неизвестным с ее банковского счета были списаны деньги.

2. Порой мошенникам даже не надо вести с вами телефонные переговоры. К вам приходит смс-сообщение с сайта, на котором вы разместили объявление о продаже, что товар забронирован. Чтобы получить за него оплату вам необходимо скачать некое приложение. Не подозревая о том, что предложенная ссылка на приложение может носить вирусный характер, активируя ее, вы подвергаете свои банковские счета доступу посторонних лиц.

Так на телефон молодой девушки поступило аналогичное смс. В результате ее действий, при попытке скачать приложение, с ее расчетного счета были списаны денежные средства в сумме около 10000 рублей.

3. Притворяясь заинтересованными покупателями, мошенники могут предложить вам даже дистанционную помощь. Убедив в необходимости проследовать к ближайшему банкомату, якобы для получения вами денежного перевода на банковскую карту за товар, мошенники дают инструкции, по осуществлению которых доверчивые граждане лишаются своих денег.

Так на телефон 64-летней женщины позвонил неизвестный с предложением приобрести продаваемую ею мебель. Незнакомец убедил пенсионерку проследовать к банкомату. После осуществления ряда операций по указанию неизвестного, женщина обнаружила, что с ее банковского счета списаны денежные средства в сумме около 15000 рублей.

4. Мнимый покупатель якобы при совершении денежного перевода на ваш банковский счет совершает оплошность, направив вам бОльшую денежную сумму, чем требуется. Соответственно вам, как порядочному человеку, необходимо вернуть разницу, переслав ее обратно. Обратитесь в банк, обслуживаемый ваш счет, и убедитесь, что это именно так, прежде чем отдать свои кровные.

В полицию с заявлением о хищении неизвестным денежных средств путем обмана обратилась 44-летняя москвичка. Женщина рассказала, что ей позвонил неизвестный мужчина, который заинтересовался ее объявлением о сдаче квартиры. Для оплаты за аренду он попросил данные ее банковской карты. Затем мужчина сообщил, что случайно перевел на ее счет бОльшую денежную сумму, чем требовалось, в связи с этим она должна обратно перевести ему разницу. Через банкомат женщина перевела денежные средства, а позже выяснилось, что денег на ее счет не поступало вовсе.

5. Являясь покупателем вас должно насторожить, если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица. Нужно понимать, что данная сделка является опасной.

В отдел полиции обратилась 29-летняя местная жительница, которая сообщила, что через сайт продаж вступила в переписку с неизвестной, которая поместила объявление на сайте о продаже духов. Неизвестная, назвавшаяся по имени и отчеству, передала свой номер банковской карты, на которую

зеленоградка перевела денежные средства в сумме 4000 руб. Получение денежных средств неизвестная подтвердила, однако после перестала выходить на связь. Впоследствии товар не был направлен адресату, и деньги не возвращены.

В другом случае 29-летняя жительница столицы, договорившись с неизвестной, поместившей объявление о сдаче в аренду дома, расположенного в Московской области, произвела через сайт оплату со своей банковской карты в сумме 4000 рублей, однако неизвестная перестала выходить на связь. О чем женщина заявила в полицию.

6. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

В полицию обратился мужчина с заявлением о хищении денежных средств в сумме более 400.000 рублей неизвестными лицами. Мужчина рассказал, что желая приобрести автозапчасти, представленные на одном из профильных сайтов, он связался с продавцом, который прислал ему на электронную почту договор, а деньги в сумме более 200000 рублей следовало перевести на банковскую карту, открытую на имя отца продавца. Что покупатель и сделал. Через некоторое время на мобильный телефон заявителя позвонила неизвестная и, представившись сотрудником банка, попросила повторить операцию перевода денежных средств, пояснив, что переведенные ранее денежные средства на счет их клиента не поступили. Уже после повторной операции перевода продавец подтвердил получение денежных средств. Однако в указанный срок товар не поступил, продавец перестал выходить на связь, денежные средства не возвращены.

7. Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца.

В отдел полиции обратился 29-летний местный житель, с заявлением о хищении неизвестным денежных средств в сумме 90000 рублей. На одном из сайтов он увидел объявление о продаже сертифицированной компьютерной

техники известного бренда. На оставленную заявку ему позвонил мужчина, представившийся менеджером фирмы, уточнив с ним некоторые моменты, молодой человек с помощью принадлежащей ему банковской карты, перевел деньги на указанную банковскую карту, принадлежащую частному лицу. Но заказ так и не поступил.

Внимательно изучайте сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

Мошенники и банковские карты

Появление банковских карт во многом облегчило жизнь людей. Теперь нам не нужно носить с собой крупные суммы денежных средств и бояться, что какой-нибудь воришка похитит кошелек. Практически все магазины принимают оплату пластиковыми картами, а если нет, то поблизости всегда есть банкомат. Но даже такой технический прогресс не гарантирует безопасность ваших сбережений. **На смену привычным для граждан «карманникам» пришли современные кибермошенники — скиммеры.**

Скиммеры - это мошенники, которые с помощью специальных устройств, считывающих информацию с банковских карт (скиммеров), путем определенных махинаций, снимают денежные средства со счетов граждан.

Как же это происходит?

Для того, чтобы узнать содержимое карты, мошенникам нужно скопировать две вещи: магнитную полосу на карте и ПИН-код. Для этого у них в арсенале три устройства.

Скиммер — миниатюрное считывающее переносное устройство, которое крепится к картридеру банкомата. Именно оно считывает всю информацию, записанную на магнитной полосе банковской карты. Получив данные, мошенники переносят их на заранее заготовленные фальшивые карты. Но без ПИН-кода они не могут реализовать свой преступный замысел, поэтому в ход идут другие снаряжения — скрытые камеры или накладные клавиатуры.

Скрытые камеры крепят на банкомат или прячут где-то рядом. Такая камера направлена на клавиатуру банкомата и записывает, как клиенты вводят ПИН-код. Также мошенники могут установить на банкомат **поддельную клавиатуру поверх оригинальной**. Она запоминает все, что вы набираете, и передает нажатия на настоящие клавиши. Банкомат реагирует на нажатия как обычно, поэтому подмену заметить сложно. Потом преступники забирают накладку, расшифровывают запись и **узнают ПИН-код**.

Стоит отметить, что мошенники списывают средства со счетов граждан обычно ночью, чтобы потерпевший не успел заблокировать карту.

Как же обезопасить свои средства от посягательств скиммеров?

- Не стесняйтесь изучить поверхность банкомата. Потрогайте панели. Обычно фальшивые держатся плохо. Если что-то шатается, изучите деталь поближе.

- Плохой сигнал — если на ровной поверхности встретилось миниатюрное углубление, которое издалека выглядит как черная точка. Присмотритесь, возможно, это глазок видеокамеры.

- У мошенников не всегда есть возможность покрасить фальшивые запчасти в цвет банкомата. Несовпадение по цвету и тону легко заметить.

- Пользуйтесь только хорошо знакомыми банкоматами. Банкоматы в отделении банков находятся под наблюдением охранников и являются более безопасными. В людных местах и местах с большой проходимостью сложнее незаметно установить скиммеры. Банкоматы, находящиеся в глухих переулках и в плохо освещенных местах, больше всего подвержены риску, поэтому старайтесь ими не пользоваться.

- Прежде чем вставить вашу карту в банкомат, внимательно осмотрите картридер на присутствие в нем посторонних предметов, накладок, наклеек, вставок. По возможности пользуйтесь банкоматами, оснащенными антискиммерами — это такие пластиковые прозрачные насадки, которые наносятся на щель, куда вставляется карта.

- Считать информацию с карты также могут в кафе или магазине. Поэтому обязательно требуйте проведения операций с картой только в Вашем присутствии.

- Присмотритесь, если банкомат старый, со сколами и затертыми панелями, а клавиатура выглядит как новая, — это признак скиммеров. Не бывает, чтобы банки меняли клавиатуру отдельно от корпуса банкомата. Если клавиатура отличается по фактуре, выпирает или шатается, попробуйте поддеть ее ногтем.

- Если банкомат атакован мошенниками, под накладкой вы увидите настоящую клавиатуру. Чаще всего лже-клавиатуру приклеивают клеем или двусторонним скотчем. Поэтому при наборе клавиш ощущается небольшой люфт. Накладка как бы «отходит» от банкомата.

- Всегда прикрывайте ладонью панель клавиатуры. Это не позволит видео камере мошенников зафиксировать искомую комбинацию вашего ПИН-кода.

- Банкоматы, имеющие на клавиатуре специальные «крылья», затрудняют установку лже-клавиатур и почти полностью исключают возможность записи ввода ПИН-кода на скрытую камеру.

- Подключите услугу "СМС-банк", тогда Вы сможете быстро среагировать на внезапные списания.

Что делать, если вам попался скимминговый банкомат?

1. Не забирайте фальш-детали, не открепляйте их.

2. Заберите вещи и уходите подальше от банкомата. Не привлекайте к себе внимание, за вами могут следить из машины или пешком.

3. Убедитесь, что за Вами не следят. Потом позвоните в банк, которому принадлежит банкомат, и сообщите о случившемся.

4. Если вы заметили скиммер уже после того, как вставили карту, оставьте ее в банкомате. Позвоните в свой банк, заблокируйте и опишите ситуацию.

Мошенники взламывают страницы в соцсетях и обманом выманивают деньги у граждан

Практически каждый современный пользователь Интернета имеет личную страничку в одной, а то и нескольких социальных сетях, где можно переписываться с друзьями, делиться фотографиями и иной информацией. Однако от граждан, пользователей той или иной социальной сети, все чаще и чаще стали поступать заявления в полицию о мошеннических действиях неизвестных лиц, которые посредством социальных сетей от имени их знакомых обманным путем завладевают денежными средствами.

В полицию обратилась 25-летняя жительница 4 микрорайона Зеленограда с заявлением о мошенничестве. Со слов девушки в одной из социальных сетей, где она имеет страницу, ей поступило сообщение от знакомого, с просьбой одолжить 8000 рублей. После перевода денег на указанный в переписке счет банковской карты, девушка позвонила знакомому, который сообщил, что денег он не просил, а его страница в соцсети взломана.

Как правило, мошенники досконально изучают взломанную страницу пользователя и пишут от его имени самым близким людям, доверие которых высоко.

В ОМВД России по районам Матушкино и Савелки г. Москвы обратилась 38-летняя женщина, она сообщила, что через социальную сеть от сына, находящегося в другом городе, получила сообщение с просьбой о переводе денежных средств на банковскую карту его товарища. Что женщина и сделала. Через несколько дней, когда женщине удалось поговорить с сыном по телефону, выяснилось, что о переводе денежных средств он не просил, а его страница взломана. Ущерб составил 4300 рублей.

В ОМВД России по району Крюково г. Москвы обратилась 36-летняя москвичка, которая сообщила, что через социальную сеть получила сообщение со страницы брата с просьбой перевести денежные средства. Откликнувшись, женщина перевела со своего счета на указанный расчетный счет 15000 рублей. Позже оказалось, что страница брата была взломана.

УВД по Зеленоградскому АО ГУ МВД России по г. Москве рекомендует гражданам при поступлении подобных сообщений даже от самых близких

друзей или родственников, перезванивать им, чтобы уточнить, действительно ли они нуждаются в вашей помощи, либо задавать собеседникам такие вопросы, ответы на которые знаете только вы и они.

Так 34-летний житель 20 микрорайона Зеленограда получил сообщение от друга, который просил перевести денежные средства в сумме 13 000 рублей на банковскую карту. Деньги заявитель не стал переводить, а тут же связался со своим другом по телефону, и тот пояснил, что его страницу взломали.

Чтобы обезопасить себя от взлома аккаунта рекомендуем придерживаться следующих правил:

- создавайте сложные пароли, используя цифры, символы, а так же прописные и заглавные буквы.

- никогда не переходите по подозрительным ссылкам, особенно если их прислали незнакомые люди.

- при входе на свою страницу, где необходимо ввести данные, всегда смотрите на адрес сайта в поисковой строке браузера, он может отличаться от оригинального знаком или одной буквой и оказаться фальшивым.

Мошенники под видом оператора сотовой связи активизировались в Свердловской области. Будьте бдительны

Злоумышленники под предлогом продления договора на оказание услуг связи отправляют потерпевшим СМС-сообщение с 4-х значным кодом, блокируют им доступ в личный кабинет на "Госуслугах" и заставляют оформлять так называемые "зеркальные кредиты" и снимать со счетов личные сбережения.

Только в Екатеринбурге за минувшие сутки по новой мошеннической схеме потерпевшие лишились свыше трех миллионов рублей. Данные факты были зарегистрированы на территориях Ленинского, Октябрьского, Верх-Исетского, Железнодорожного районов Екатеринбурга и в ряде муниципалитетов области.

По всем фактам хищения денежных средств возбуждены уголовные дела по статье "Мошенничество". Сотрудники органов внутренних дел

предпринимают комплекс оперативно-розыскных мероприятий, направленных на раскрытие данных преступлений.

Как пояснили сами потерпевшие, им звонили неизвестные, представлялись "сотрудниками сотовых операторов" и говорили о необходимости продления договора на оказание услуг связи. Затем заявителям по СМС приходил 4-х значный код, который они передавали звонившим. После этого, неизвестные вдруг заявляли, что они являются мошенниками, страницы граждан на сайте "Госуслуг" взломаны, и они занимаются оформлением на них кредитов. Растерянные свердловчане пытались зайти в личный кабинет "Госуслуг", но их доступ в приложение был заблокирован, и для его восстановления нужно было обратиться в контактный центр, номер которого высвечивался во всплывающем на экране окне. Когда заявители звонили по данному номеру, их соединяли с псевдосотрудниками банка, которые заверяли граждан, что от их имени поданы заявки на получение кредитов, и с целью предотвращения мошеннических действий необходимо самостоятельно оформить "зеркальные займы". Затем потерпевших переключали на лжеследователей, которые подтверждали слова липовых финансистов и убеждали жертв, что по факту мошенничества проводится расследование, и они не должны никому сообщать данную информацию.

В итоге, потерпевшие под мощным психологическим давлением псевдопровайдеров, "силовиков" и "сотрудников банков" согласились выполнить их требования и перевели на указанные ими "безопасные счета" свыше трех миллионов кредитных и личных средств.

Официальный представитель Свердловского главка МВД Валерий Горелых призвал граждан быть более бдительными и не под каким предлогом не переводить свои деньги на неизвестные счета. Все, что нужно сделать в таких ситуациях - немедленно закончить разговор и обратиться органы внутренних дел.

Полковник Горелых напомнил, что сотрудники полиции, ФСБ, прокуратуры, СКР и других ведомств, а также представители банков никогда не звонят горожанам по вопросам перевода денег на «безопасные счета».