Как не стать жертвой «мобильного» мошенничества

Злоумышленники могут обратиться к Вам:

- под видом сотрудников полиции, о нарушении их близкими родственниками законов, с целью передачи Вами денежных средств через посредников, либо перевод их через терминалы оплаты для разрешения сложившейся ситуации.

Не продолжайте разговор, не позволяйте себя убедить. Вам звонит мошенник. Обратитесь в полицию!

- о блокировке банковской карты путем рассылки SMS-сообщений, а так же о переводе денежных средств за покупку товара по объявлению и последующего информирования о необходимости дальнейшего введения ряда команд с банкомата.

Вам звонит мошенник. Не предоставляйте злоумышленникам сведения о Вашей карте. Обратитесь в банк, обслуживающий Вашу банковскую карту, в банке решат Вашу проблему.

- о сообщении Вам, якобы, из поликлиники или больнице, что у Вас или у Ваших родственников обнаружили страшный диагноз и чтобы вылечить болезнь необходимо перевести деньги за лекарства.

Прервите разговор. Вам звонит мошенник. Медицинское учреждение принимает денежные средства после заключения соответствующего договора в письменном виде, при Вашем личном присутствии. Свяжитесь с Вашим родственником, позвоните в больницу. Не переводите денежные средства мошенникам. Обратитесь в полицию!

- получения СМС-сообщений с неизвестных номеров о выигранном призе, с просьбой положить деньги на телефон, или вернуть деньги, так как они были переведены ошибочно.

Это обман. Не отвечайте на сообщение, не присылайте информацию по

карте и не переводите денежных средств.

1.

Никому нельзя сообщать реквизиты своей банковской карты, в том числе сотруднику банка, об этом всегда информируют банк при получении пароля к карте, в последствие необходимо лично обратиться в ближайшее отделение банка, с целью выяснения возникших проблем с банковской картой.

2.

Различные компенсации выплачиваются гражданам только при их личном письменном обращении, никаких процентов за выплату компенсаций платить не надо.

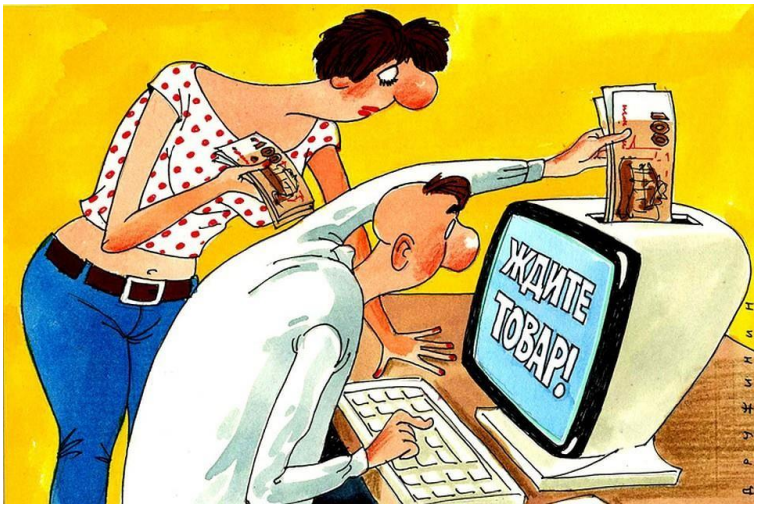
3.

Настоящий врач никогда не будет звонить Вам по телефону и сообщать о страшном диагнозе или просить перевести деньги за лекарства.

4.

В случае получения СМС-сообщений с неизвестных номеров, помните это мошенники, человек не может выиграть приз не участвуя в лотереях, родственники не будут Вам высылать СМС-сообщения с неизвестных номеров.

Как не стать жертвой мошенничества, используя сеть Интернет



Злоумышленник, с целью хищения Ваших денежных средств, размещает в сети Интернет объявление о продаже какого-либо объекта (телефон, машина, квартира) по заниженной цене и оставляет свои контактные данные.

После того, как Вы собираетесь приобрести товар, связываетесь с мошенником, он сообщает, что для покупки необходимо внести предоплату (на расчетный счет, счет, яндекс - деньги, счет вебмани и т.д.).

Наиболее часто встречающимися площадками для размещения подобных объявлений является сайты социальных сетей **«Вконтакте», «Instagram», «Одноклассники»,** также такими сайтами могут выступать ресурсы бесплатных объявлений **«Авито», «Юла» и «auto.ru».** Злоумышленник объясняет внесение предоплаты тем, что живет в другом регионе и отправит товар сразу после того, как удостовериться уплате за товар. Злоумышленник может выслать копию паспорта (поддельную).

Также, распространенным способом мошенничества в сети интернет, является создание сайтов интернет-магазинов. Злоумышленник по электронной почте высылает договор, который заполняет заказчик, после чего просит внести предоплату за товар.

Также встречается создание сайтов-клонов на которых искажены реквизиты получателя. Сайты клоны создаются, таким образом, что пользовательский интерфейс является копией оригинального Интернет-ресурса. Различие может заключаться только в доменном имени (например оригинальный ресурс «tech-point.ru» и сайт двойник «tex-point.ru»).

- редко какой-либо интернет-магазин работает по предоплате, зачастую товар на дом привозит курьер, только после осмотра и проверки товара продавец платит деньги;

- прежде чем заказать товар в Интернете, почитайте отзывы на разных сайтах о данном интернет-магазине или виртуальном продавце, как правило, Вы сразу обнаружите отрицательные отзывы, отсутствие отзывов о выбранном Вами интернет-магазине (говорит о коротком периоде его существования),:

- внимательно читайте названия Интернет-магазина, пробуйте зайти на данный Интернет-магазин с разных сайтов, тем самым Вы сразу

обнаружите сайты-клоны;

- старайтесь избегать покупки товара по предоплате;

- цена товара гораздо ниже цены как в обычных розничных магазинах, так и в других интернет-магазинах, либо на рынке в целом (например, при продаже автомашины по заниженной стоимости);

- требование продавцом внесения предоплаты за товар (зачастую - 100%);

- запрос покупателем, якобы для перечисления предоплаты, либо оплаты за товар информации не только о шестнадцатизначном номере карты (требуется исключительно только он), но и сроке ее действия, данных владельца и трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты – CVV или CVC коды (не путать с ПИН-кодом, необходимым для доступа к терминалам (банкоматам)), с последующей необходимостью сообщения пришедшего на абонентский номер владельца карты кода подтверждения операции.

Как не стать жертвой мошенничества с банковскими картами

При использовании услуги «Мобильный банк»:

В случае потери мобильного телефона с подключенной услугой «Мобильный банк» или мобильным приложением «Сбербанк Онлайн» **следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный центр Банка для блокировки услуги «Мобильный банк» и/или «Сбербанк Онлайн».**

При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение), с целью отключения услуги «Мобильный банк» от старого номера и подключения на новый.

Не следует оставлять свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг другими лицами.

Не подключайте к услуге «Мобильный банк» абонентские номера, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Банка.

При пользовании банковскими картами:

С целью избежания несанкционированных действий с использованием карты, необходимо требовать проведения операций с ней только в Вашем присутствии, никогда не позволять уносить третьим лицам карту из поля Вашего зрения.

В случае обращения кого-либо лица лично, по телефону, в сети «Интернет», через социальные сети или другим способом, которое под различными предлогами пытается узнать полные данные о вашей банковской карте: шестнадцатизначном номере, сроке действия, данных владельца, трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты и т.д. (паролях или другой персональной информации), **будьте осторожны - это явные признаки**

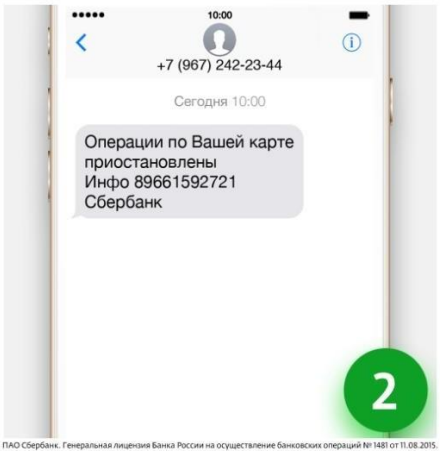
противоправной деятельности. При любых сомнениях рекомендуется прекратить общение и обратиться в банк по телефону, указанному на обратной стороне банковской карты.

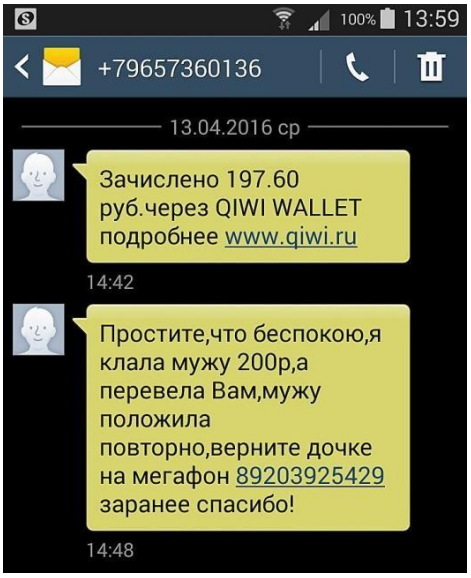
Не следует прислушиваться к советам третьих лиц, а также отказаться от их помощи при проведении операций. В случае необходимости, обращаться к сотрудникам филиала банка или позвонить по телефонам, указанным на устройстве или на обратной стороне карты.

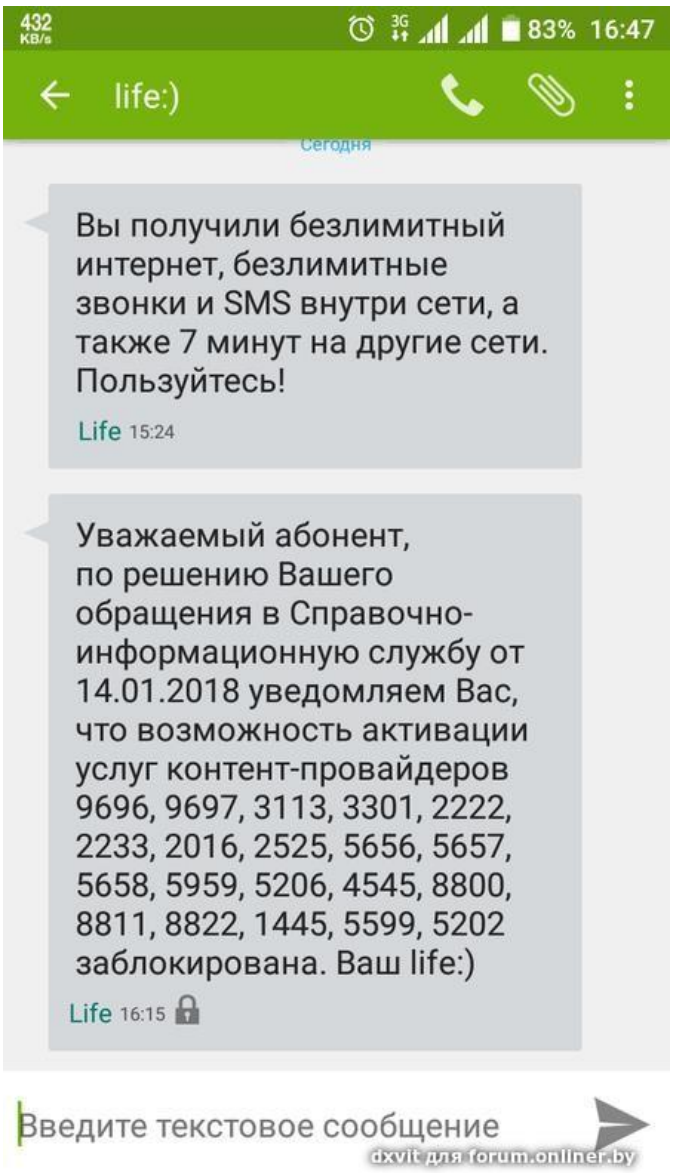
Во избежание использования карты другим лицом, следует хранить ПИН-код отдельно от карты, не писать ПИН-код на карте, не сообщать ПИН-код другим лицам (в том числе родственникам).

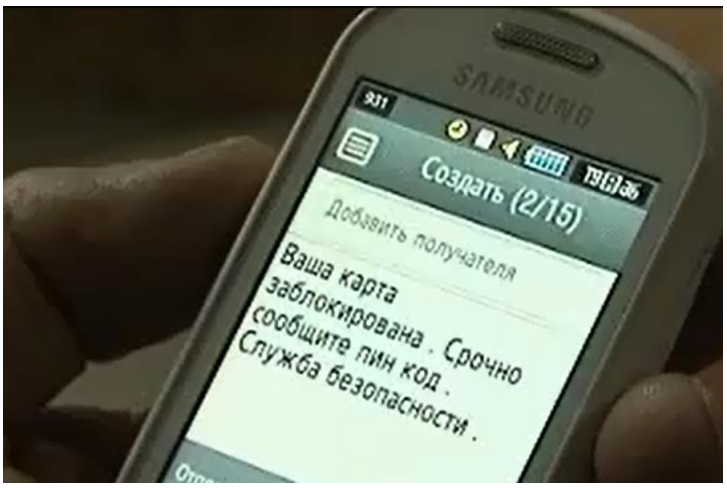
Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие поSMS/MMS/электронной почте/мессенджерам (Вайбер, ВацАп и др.), в том числе от имени Банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.

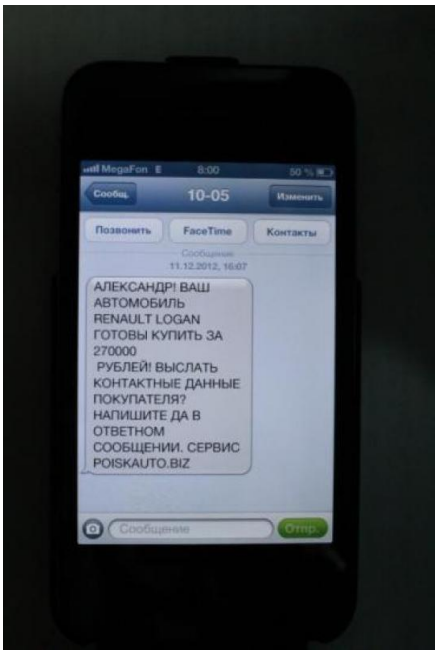
НЕ ВЕРЬТЕ ПОДОБНЫМ СООБЩЕНИЯМ, НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ, НЕ ОТВЕЧАЙТЕ НА СООБЩЕНИЯ.

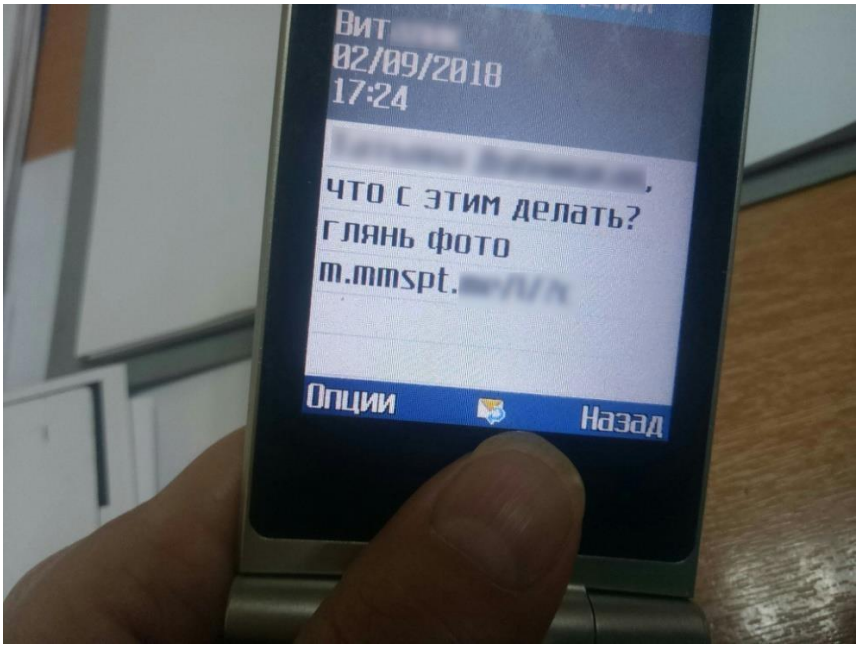




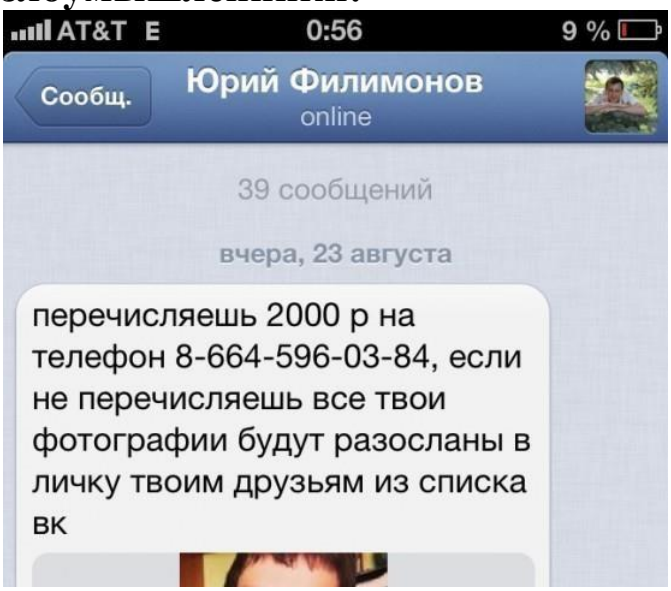

432 KB/s
83% 16:47
life:)
Сегодня
Вы получили безлимитный интернет, безлимитные звонки и SMS внутри сети, а также 7 минут на другие сети. Пользуйтесь!
Life 15:24
Уважаемый абонент, по решению Вашего обращения в Справочно-информационную службу от 14.01.2018 уведомляем Вас, что возможность активации услуг контент-провайдеров 9696, 9697, 3113, 3301, 2222, 2233, 2016, 2525, 5656, 5657, 5658, 5959, 5206, 4545, 8800, 8811, 8822, 1445, 5599, 5202 заблокирована. Ваш life:)
Life 16:15
Введите текстовое сообщение
dxvit для forum.onliner.by


SAMSUNG
Создать (2/15)
Добавить получателя
Ваша карта заблокирована . Срочно сообщите пин код . Служба безопасности .


MegaFon
8:00
50 %
Сообщ.
10-05
Изменить
Позвонить
FaceTime
Контакты
Сообщение
11.12.2012, 16:07
АЛЕКСАНДР! ВАШ АВТОМОБИЛЬ RENAULT LOGAN ГОТОВЫ КУПИТЬ ЗА 270000 РУБЛЕЙ! ВЫСЛАТЬ КОНТАКТНЫЕ ДАННЫЕ ПОКУПАТЕЛЯ? НАПИШИТЕ ДА В ОТВЕТНОМ СООБЩЕНИИ. СЕРВИС POISKAUTO.BIZ
Сообщение
Отпр.


Вит
02/09/2018
17:24
что с этим делать?
глянь фото
m.mmspt.
Опции
Назад

Если Вы ведете переписку в сети Интернет («В Контакте», «Одноклассники» и др.), если Вы общаетесь с кем то, используя сайт знакомств, будьте бдительны! Не присылайте незнакомцам Ваши личные фото. Вашим доверием могут воспользоваться злоумышленники!



Телефоны 102, 112.

Телефон доверия ГУ МВД России по Волгоградской области 30-44-44

Телефон дежурной части ГУ МВД России по Волгоградской области
30-43-45.