ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомни основные схемы и признаки популярных мошенничеств! Эта информация поможет вовремя распознать злоумышленников.

Распространение вредоносного программного обеспечения (вирусов)

ПРИЗНАКИ

1. **На телефон поступает сообщение** от абонента из списка контактов в Вашей телефонной книге с предложением открыть прилагаемую **интернет-ссылку**, чтобы, например, посмотреть фото

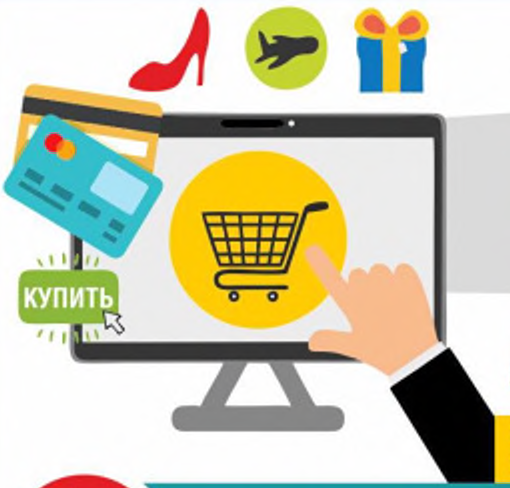
2. Если Вы откроете ссылку, Ваш т**елефон может перезагрузиться или вовсе выйти из строя.**

ЗАПОМНИТЕ:

Ни в коем случае **не открывайте интернет-ссылки**, полученные по **смс** или в **мессенджерах даже от собственных знакомых!** Пройдя по ним, можно **загрузить вредоносную программу** в свой мобильный телефон. Если **сим-карта** подключена к Вашему **«мобильному банку»,** произойдет **списание денег со счета.**

Зараженный телефон может автоматически **рассылать аналогичные ссылки** всем абонентам из списка контактов в Вашей телефонной книге.

42.мвд.рф



ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомни основные схемы и признаки популярных мошенничеств!
Эта информация поможет вовремя распознать злоумышленников.

ПОКУПКА/ПРОДАЖА ТОВАРОВ через сайты объявлений

ПРИЗНАКИ

1. **Низкая стоимость** товара
2. Требование **безналичного расчета**
3. Предложение подключить **«мобильный банк»**
4. Покупатель готов сделать покупку, **не взглянув на нее**
5. Покупатель просит назвать **реквизиты банковской карты и пароли из СМС-сообщений**
6. Продавец под разными предлогами просит вас внести **предоплату**
7. Покупатель **предлагает обмен** и высылает по СМС **вредоносную ссылку** якобы на товар

ЗАПОМНИТЕ:

Главная цель злоумышленников – **ПОДКЛЮЧИТЬСЯ К ВАШЕМУ «МОБИЛЬНОМУ БАНКУ»!**

ДЛЯ СОВЕРШЕНИЯ ДЕНЕЖНОГО ПЕРЕВОДА НЕОБХОДИМО ЗНАТЬ ТОЛЬКО НОМЕР БАНКОВСКОЙ КАРТЫ

Если покупатель предложил **ПРОЙТИ К БАНКОМАТУ** для получения перевода, знайте: **ВАС ПЫТАЮТСЯ ОБМАНУТЬ!**

НЕ ОТКРЫВАЙТЕ ИНТЕРНЕТ-ССЫЛКИ от покупателя, они могут быть вредоносны!

42.мвд.рф

ПОЛИЦИЯ КУЗБАССА ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО!

МОШЕННИКИ!

Звонок от «сотрудника банка»

ПРИЗНАКИ

1. поступление звонка от «сотрудника банка» (специалиста, работника службы безопасности);
2. сообщение о попытке хищения денежных средств;
3. предложение заблокировать несанкционированную операцию либо перевести денежные средства на «безопасный» счет;
4. просьба назвать реквизиты банковской карты, защитный код с ее обратной стороны и поступающие на телефон пароли.

ЗАПОМНИТЕ!

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;

НЕ ВЕРЬТЕ любой информации от незнакомца, **ДАЖЕ ЕСЛИ** звонок поступил с официального телефона горячей линии банка;

ПРЕРВИТЕ РАЗГОВОР и самостоятельно позвоните на телефон горячей линии банка, набрав номер **ВРУЧНУЮ**;

ПОМНИТЕ: код от вашей карты и пароли подтверждения операций **НЕ ИМЕЕТ ПРАВА** спрашивать даже сотрудник банка!

42.мвд.рф

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомни основные схемы и признаки популярных мошенничеств!
Эта информация поможет вовремя распознать злоумышленников.

КОМПЕНСАЦИЯ за приобретенные лекарства (БАДы)

ПРИЗНАКИ

1. **Поступление телефонных звонков**, начинающихся, преимущественно, с цифр **«8-495...», «8-499...», «8-812»**
2. Собеседник представляется работником **правоохранительных органов** и сообщает, будто Вам полагается **компенсация за** ранее приобретенные **медицинские препараты или БАДы**
3. Собеседник пытается убедить Вас, что **для получения денег необходимо оплатить НДС, страховку и т.д.**

ЗАПОМНИТЕ!

КОМПЕНСАЦИЯ за ранее приобретенные лекарства или БАДы - это стандартная **УЛОВКА МОШЕННИКОВ!**

НЕ ПРИОБРЕТАЙТЕ медицинские препараты или добавки **ЧЕРЕЗ ИНТЕРНЕТ** и не заказывайте их **ПО ТЕЛЕФОНУ**. Любой курс терапии назначается только лечащим врачом!

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ по просьбе незнакомцев, кем бы они ни представлялись!

42.мвд.рф

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомни основные схемы и признаки популярных мошенничеств! Эта информация поможет вовремя распознать злоумышленников.

«Родственник в беде»

ПРИЗНАКИ

1. Неизвестный звонит на телефон, представляется, как правило, **сыном или внуком,** и говорит, **будто совершил ДТП или преступление**, в результате которого пострадал человек
2. Собеседник передает телефонную трубку якобы **сотруднику правоохранительных органов**, который пытается убедить Вас, что для избавления родственника от уголовного преследования **необходимы деньги**
3. Собеседник **пытается удержать Вас на связи** любыми способами, чтобы не дать возможность положить трубку

ЗАПОМНИТЕ:

Задайте собеседнику **вопрос**, ответ на который может знать только близкий Вам человек

Прервите разговор и **перезвоните родным**, чтобы убедиться, что с ними все в порядке

Если собеседник представляется работником правоохранительных органов, попросите его **назвать фамилию, имя, отчество, а также должность и место службы.** Позвоните в соответствующее ведомство и узнайте, действительно ли в нем работает такой сотрудник.

Помните, что **передача денежных средств должностным лицам** за незаконные действия или бездействие является **уголовно наказуемым деянием**

42.мвд.рф

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомните основные схемы и признаки популярных мошенничеств! Эта информация поможет вовремя распознать злоумышленников.

Взлом (дублирование) страниц пользователей в социальных сетях

ПРИЗНАКИ

1. В социальной сети от пользователя из **списка Ваших друзей** поступает сообщение с **просьбой одолжить денежные средства** либо предложением **принять участие в акции** банка и получить гарантированный денежный приз
2. Под этими предлогами собеседник просит назвать **реквизиты банковской карты и пароли из СМС-сообщений**

ЗАПОМНИТЕ:

Отличить настоящую страницу пользователя в соцсети **от ее дубликата**, созданного мошенниками, внешне практически **невозможно**! Поэтому обязательно **перезвоните человеку**, от имени которого Вам поступило сообщение, и уточните достоверность информации.

Реквизиты банковской карты являются конфиденциальной **информацией ее владельца**, как и **уведомления банка с паролями**, необходимыми для подтверждения той или иной операции.

Защитите от взлома свои аккаунты в социальных сетях при помощи **надежного пароля,** который необходимо держать **втайне** от окружающих.

42.мвд.рф

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомни основные схемы и признаки популярных мошенничеств!
Эта информация поможет вовремя распознать злоумышленников.

Преступления, совершаемые лицами ЦЫГАНСКОЙ народности

ПРИЗНАКИ

1. **Попытка попасть в ваше жилище** под видом работника ЖКХ, врача или сотрудника социальных служб, а также под предлогом покупки жилья, предоставления ночлега
2. Предложение **обмена «старых» денег** на «новые» или получения **доплат к пенсии**
3. **Предложение купить** дешевые мед, посуду, уголь, одежду
4. **Предложение снятия «порчи»**, проведение ритуалов с использованием швейных игл, куриных яиц, «червей», «живой» или святой воды
5. **Просьба одолжить деньги** якобы для оформления груза на таможне, обещание вернуть долг «с процентами»

ЗАПОМНИТЕ:

Никогда **не открывайте дверь незнакомцам** и не впускайте посторонних в свою квартиру или дом!

Не показывайте и не передавайте деньги и ювелирные украшения посторонним!

Избегайте общения с теми, кто **предлагает купить дешевые товары** или продукты питания, погадать либо **снять порчу!**

Обращайте внимание на денежные купюры, получаемые из рук незнакомцев. Надпись **«Купюра банка приколов»** означает, что она **сувенирная**!

42.мвд.рф

ПОЛИЦИЯ КУЗБАССА ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО!

МОШЕННИКИ!

Звонок от «брокера»

ПРИЗНАКИ

1. поступление звонка от «представителя брокерской компании»;
2. предложение быстрого обогащения за счет торговли на финансовых рынках;
3. предоставление системы «безрискового трейдинга»;
4. просьба установить на телефон или компьютер специализированного программного обеспечения, зарегистрироваться и внести предоплату;
5. неоднократные требования пополнения счета либо перевода денежных средств на сторонние счета;
6. блокировка счета клиента, отсутствие реальной возможности вывода денег.

ЗАПОМНИТЕ!

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;

НЕ ВЕРЬТЕ любой информации о быстром обогащении;

НЕ ПЕРЕВОДИТЕ свои деньги на сторонние счета;

ПРЕРВИТЕ РАЗГОВОР и сообщите о произошедшем в полицию!

42.мвд.рф

Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

-Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;

-Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;

-Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные;

-Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

-Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;

-Сотрудник банка может запросить у клиента только контрольное слово, ФИО;

-При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;

-Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

-При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

-Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

-Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

-Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Памятка безопасности при онлайн-покупке товаров и онлайн-оплате услуг

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категорий товаров по ценам значительно НИЖЕ, чем среднерыночная цена.

Злоумышленники:

-Создают сайт интернет-магазина и запускают рекламный трафик с целью появления в топе поисковых систем;

-Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина;

-Требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен;

-После перевода денежных средств покупателем перестают выходить на связь, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

-неоправданно низкая цена на товар;

-электронная почта или мессенджеры в качестве способов коммуникации;

-оплата без расчетного банковского счета, отсутствие наименования организации в любой из форм собственности;

-обязательная предоплата, зачастую более половины стоимости товара;

-отсутствие физического адреса расположения магазина или его несоответствие данным интерактивных карт;

-сомнительный интернет-адрес.

Запомните!

-Необходимо выбирать магазин, предлагающий забрать товар самовывозом. При необходимости закажите доставку товара;

-Самый безопасный способ оплаты - после получения заказа;

-Критично относитесь к ситуации, когда менеджер интернет-сайта проявляет излишнюю настойчивость или просит немедленно оплатить заказ под различными предлогами (акционный товар, последний экземпляр, ожидается подорожание продуктовой линейки).

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Мошенничество с использованием сайтов-дублеров благотворительных организаций

В сети интернет регулярно размещаются объявления от лица благотворительных организаций, детских домов, хосписов, приютов и др. с просьбой о материальной помощи.

Злоумышленники:

-Создают сайт-дублер, являющийся точной копией оригинального;

-Меняют реквизиты для перечисления денежных средств.

Запомните!
Прежде чем помочь какой-либо организации:

-Позвоните по телефону в указанную организацию;

-Уточните номер расчетного счета, либо посетите ее лично;

-Убедитесь в достоверности размещенной информации.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.