чено, закон защищает ваши права. Взять хотя бы те самые ночные звонки. За них коллектора, звонившего вам, можно привлечь к административной ответственности. Угрозы и вымогательство – это и вовсе уголовно наказуемые преступления.

Пишите в СМИ

Если не знаете, как бороться с коллекторами самостоятельно – ищите помощь извне! Ведь есть множество газет, аудитория которых могла бы узнать о вашей проблеме. Помимо того, что такой опыт помог бы другим людям, вы также несколько накажете агентство, с которым работали.

Как погасить долг?

Еще один важный совет, который вы обязательно должны учитывать – это форма и способ возврата денег, взятых в банке. Как показывает практика, коллекторы очень часто требуют выплаты в наличной форме, адресованной непосредственно сотрудникам. Из-за этого, случается так, что растерянный должник просто отдает свой долг на руки работнику. Думаю, не стоит уточнять, что происходит с этими средствами далее: ясно, что долг они не погашают. Расчитываться с банком нужно только по тем реквизитам, которые указаны в кредитном договоре. Вы не должны менять форму и способ оплаты только из-за того, что этого требует коллектор. Только если вы оплатите по счетам из договора, вы сможете, во-первых, доказать что-то в суде в случае, если платеж не засчитают; во-вторых, будете уверены в том, что изначальный кредитор получил ваши средства.

https://businessman.ru/new-kak-borotsya-s-kollektorami-sovety-yuristov.html

ВИДЫ ОПЛАТЫ. ЗАЩИТА ОТ МОШЕННИКОВ

КАКИЕ БЫВАЮТ СПОСОБЫ ОПЛАТЫ?

Современные способы оплаты товаров и услуг просто поражают воображение. Не трудно представить, что в скором времени мы будем оплачивать продукты в одно касание пальцем какого-нибудь считывающего устройства. Конечно, все это фантазии, а пока поговорим о возможных способах оплаты и их классификации.

Платежи на территории РФ могут осуществляться наличными или безналичными расчетами. Это основная классификация, которая разделяет абсолютно все способы платежей.

Платеж наличными – вид расчетов, при котором оплата товара или услуги производится посредством передачи наличных денег от одного лица другому.

Безналичный расчет – вид платежа, при котором оплата товара осуществляется без применения наличных денег, вместо этого средства вносят на банковский счет, электронный кошелек и т.д.

Способы оплаты наличными:

- Наличными в кассе, курьеру, путем передачи денежных средств от непосредственного заказчика исполнителю или третьему лицу.
- Через терминалы самообслуживания Qiwi, Элекснет, Киберплат и другие. Пользователь выбирает необходимую услугу на экране терминала и оплачивает ее, путем внесения денежных средств в купюроприемник. В таких терминалах можно оплатить практически все, в том числе кредиты, онлайн-займы и т.д.
- В банковских ПВН и банкоматах с функцией приема наличных. Опять же нужно выбрать необходимый параметр (например, оплата госпошлины), ввести назначение платежа и вставить купюры, оплатив операцию.
- Платеж в банке или на Почте России. Большинство пенсионеров до сих пор платят за электроэнергию и квартиру в отделениях Почты, так уж завелось. Для совершения платежа необходимо предъявить платежное поручение или просто указать реквизиты получателя, после чего передать наличные денежные средства операционисту.
- Достаточно популярным в России служит платеж через систему переводов (Contact, Лидер, Золотая Корона и т.д.) Для расчета достаточно подойди в отделение выбранной системы переводов, указать реквизиты платежа или хотя бы назвать организацию и внести наличные.

Безналичные платежи в свою очередь делятся на контактные и бесконтактные:

- Расчет с помощью банковской карты с магнитной полосой и/или чипом – самый популярный способ безналичного платежа. В последнее время карты с магнитной полосой стали вытесняться более защищенным чипованным пластиком. Чтобы оплатить товар с помощью карточки, нужно вставить ее в чип-ридер POS-терминала (для карт с чипом) или провести пластиком через ридер (для карт с магнитной полосой). После этого останется ввести ПИН-код и деньги спишутся со счета, а товар будет успешно оплачен.
- Расчет с помощью карты с технологией PayPass (Мастеркард) или Pay Wave (Visa) – самый распространенный способ бесконтактной оплаты товаров. Для расчета по такой карте достаточно поднести ее к POS-терминалу и товар автоматически будет оплачен без ввода ПИН-кода и прочих манипуляций. У этого способа есть один существенный недостаток, платеж по 1 операции не может превышать 1000 рублей. То есть, если сумма вашей покупки составит 1035 рублей, оплатить ее картой бесконтактным способом не получится, придется вставлять пластик в терминал и вводить ПИН-код. Также далеко не в каждом магазине есть терминалы с возможностью бесконтактной платы.
- Расчет с помощью реквизитов карты – еще один популярный способ бесконтактных расчетов, чаще всего применяется при оплате покупок в интернет-магазинах или услуг через интернет. Для совершения операции достаточно ввести в нужные поля номер карточки, срок ее действия, имя и

фамилию латинскими буквами, а также защитный CVC/CVV2 код, который расположен на обратной стороне пластика. После ввода необходимых реквизитов нужно вписать специальный 3D-Secure код для подтверждения операции. После чего деньги спишутся со счета.

- Платеж электронными деньгами через интернет-кошелек QIWI, Webmoney, Яндекс.Деньги и т.д. Для оплаты товаров/услуги достаточно зайти в личный кошелек одной из платежных систем и оплатить выставленный счет или просто перевести деньги по реквизитам организации и т.д.
- Оплата мобильным телефоном с технологией NFC – далеко не самый распространенный в России способ бесконтактной платы за товары/услуги. Технология NfC позволяет оплачивать различные услуги с помощью поднесения к считывающему устройству мобильного телефона. Чтобы воспользоваться этим способом, нужно приобрести сим-карту с поддержкой технологии NfC и установить в телефон дополнительную антенну. После чего можно оплачивать услуги в одно касание, просто приложив смартфон к терминалу и деньги спишутся со счета мобильника (с баланса). Конечно, в России не так много мест, где можно расплатиться по такой технологии. Например, этим методом можно воспользоваться при оплате проезда в Московском Метрополитене.
- Банковский перевод через интернет-банкинг. Еще одни способ безналичной платы за услуги. Для расчета достаточно зайти в интернет-банк, выбрать нужную категорию, ввести назначение платежа и выбрать карту/счет для списания средств в счет платы. Останется подтвердить операцию специальным кодом и деньги спишутся со счета.

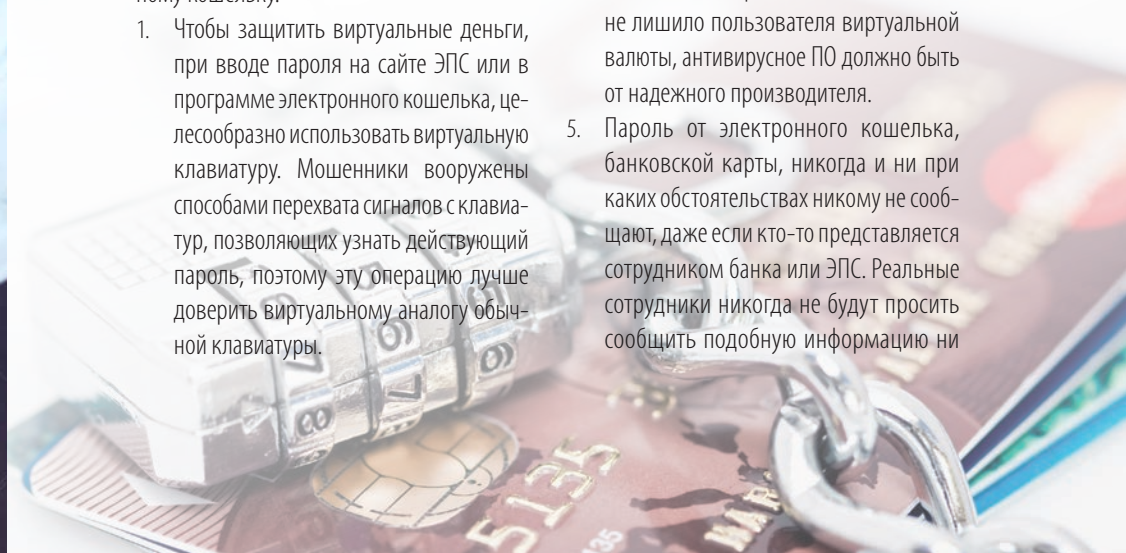
КАК МАКСИМАЛЬНО ОБЕЗОПАСИТЬ ЭЛЕКТРОННЫЕ ПЛАТЕЖИ

Проблема мошенничества приобрела актуальность ещё на начальном этапе становления интернета. Виртуальные злоумышленники используют личную информацию из социальных сетей, взламывают электронную почту, воруют пароли. Главная цель киберпреступников – получение доступа к виртуальным кошелькам.

Разработчики вкладывают солидные деньги в обеспечение сохранности электронных платежей. Однако решающую роль в сохранности своего виртуального кошелька играет сам пользователь. Постоянное улучшение механизмов защиты не может служить панацеей, если владелец электронного портмоне не соблюдает элементарные правила безопасности.

Рассмотрим правила, позволяющие максимально обезопасить электронные платежи. Они весьма простые, но не позволяют мошенникам получить доступ к электронному кошельку.

1. Чтобы защитить виртуальные деньги, при вводе пароля на сайте ЭПС или в программе электронного кошелька, целесообразно использовать виртуальную клавиатуру. Мошенники вооружены способами перехвата сигналов с клавиатур, позволяющих узнать действующий пароль, поэтому эту операцию лучше доверить виртуальному аналогу обычной клавиатуры.
2. Заходя в личный кабинет ЭПС, необходимо убедиться, что адресная строка браузера показывает необходимый сайт. Чтобы не попасть на мошеннический ресурс, нужно проверить наличие символов https. Стоящая последней буква S сообщит о наличии защиты, а, значит, пользователь попадет именно на сайт электронной платежной системы.
3. Чтобы доступ к электронным деньгам имел только их собственник, пароль должен быть максимально сложным. Это затруднит взлом виртуального кошелька при использовании специальных программ, способных перебирать много вариантов паролей для входа в кошелек пользователя.
4. Чтобы держать в сохранности электронные деньги, необходимо как можно чаще устанавливать новую версию антивирусного программного обеспечения и проводить необходимые проверки своего компьютера с требуемой периодичностью. Вирусы наиболее часто взламывают кошельки. Чтобы подобное электронное мошенничество не лишило пользователя виртуальной валюты, антивирусное ПО должно быть от надежного производителя.
5. Пароль от электронного кошелька, банковской карты, никогда и ни при каких обстоятельствах никому не сообщают, даже если кто-то представляется сотрудником банка или ЭПС. Реальные сотрудники никогда не будут просить сообщить подобную информацию ни



по телефону, ни по электронной почте. Их может требовать только злоумышленник.

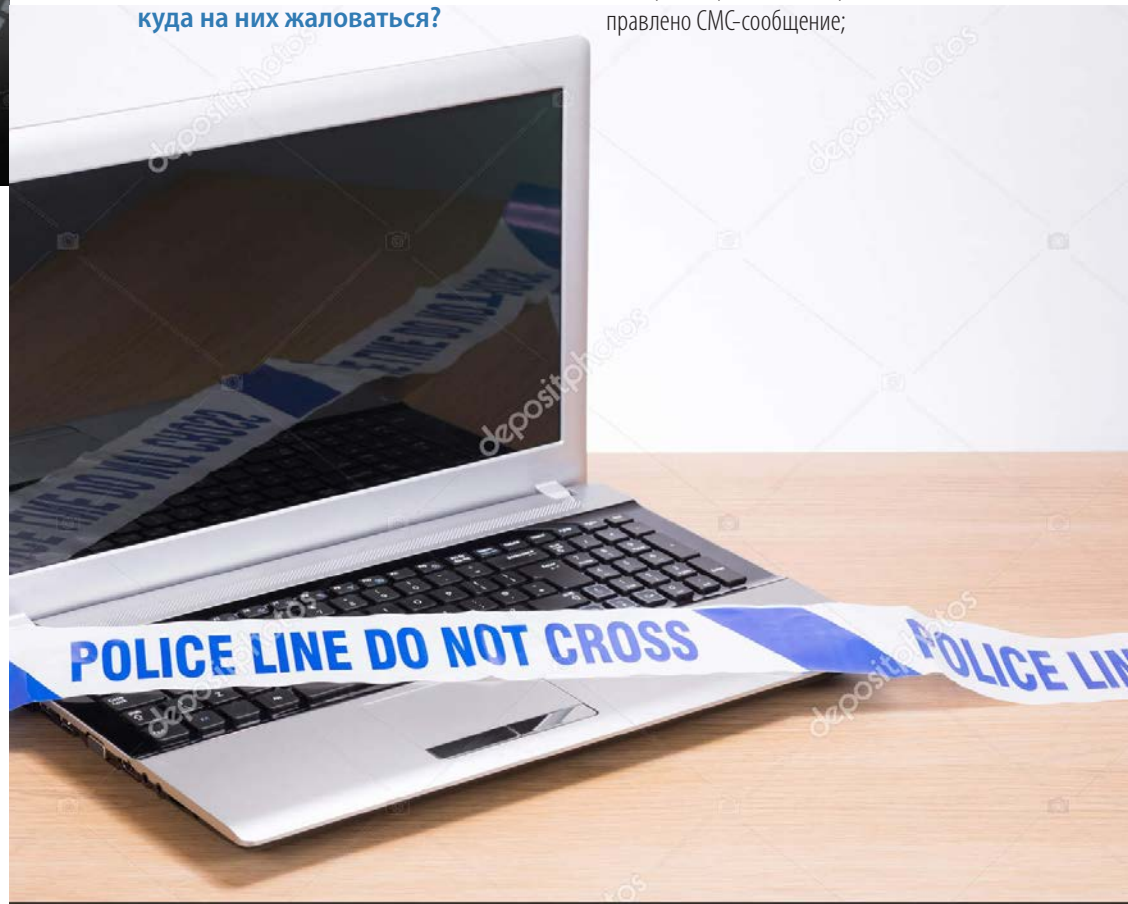
6. Вредные программные обеспечения (вирусы) открывают мошенникам доступ к компьютерам пользователей и позволяют скачивать необходимые данные. Старайтесь, не хранить пароли в электронном виде на рабочем компьютере. Используйте для этого флешку или другие альтернативные носители памяти и надежно прячьте их от посторонних людей.
7. Коды протекции, ещё один эффективный метод, позволяющий защитить деньги. Практически все ЭПС предлагают клиентам подобный сервис. Всегда используйте подобную защиту переводов, в этом случае никому не удастся перехватить переводимые деньги. Ведь защитный код протекции знает только отправитель и получатель.
8. Кричащие заголовки, например, «1000% за пару дней», «Выгодное предложение», подозрительные акции и конкурсы, чаще всего, скрывают различные мошеннические схемы. Они направленные на то, чтобы лишить доверчивых пользователей виртуальных накоплений. Под такой рекламой, как правило, скрываются финансовые пирамиды, «волшебные кошельки», недобросовестные ресурсы по обмену валют в режиме онлайн.
9. После окончания работы с электронной платежной системой лучше всего выйти из аккаунта.
10. Привязка виртуального кошелька к IP адресу значительно усилит безопасность аутентификации пользователя. Много платежных интернет-систем предоставляют такую возможность и этим надо пользоваться, потому что войти в аккаунт ЭПС можно будет только с указанной точки доступа в интернет.

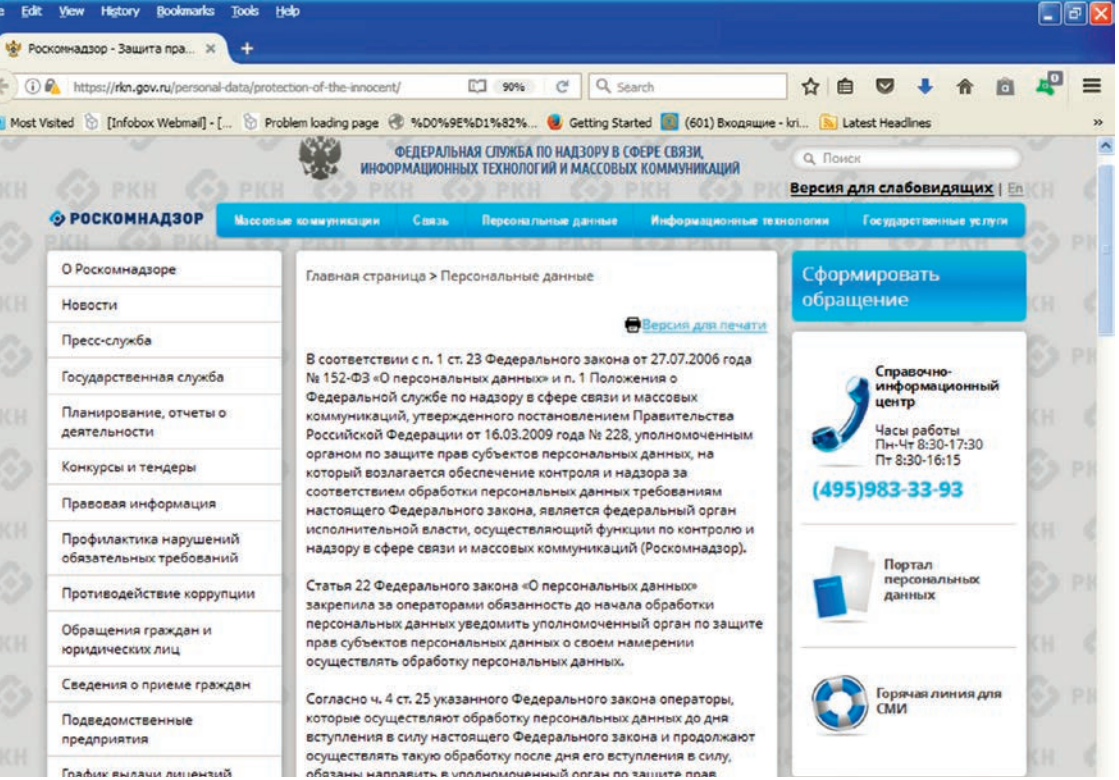
Мошенники в Интернете – куда на них жаловаться?

Всеми делами, связанными с компьютерной информацией, в системе МВД занимается отдел «К». Для более быстрого реагирования можно подать заявление непосредственно в региональное управление «К».

При написании заявления нужно указать все имеющиеся у вас данные о мошенниках, в частности:

- адрес мошеннического сайта;
- ник злоумышленника на форуме;
- номер счета или электронного кошелька, на который были переведены денежные средства;
- номер телефона, на который было отправлено СМС-сообщение;





- адрес электронной почты мошенника и т. д.

Подать жалобу на мошенничество в Интернете можно и в электронном виде – на сайте МВД. Для этого нужно заполнить специальную форму в разделе «Прием обращений». В таком случае жалобу следует адресовать непосредственно управлению «К».

Куда можно обращаться помимо полиции?

В случае если деньги были перечислены мошеннику через электронную платежную систему (например, WebMoney), стоит обратиться в службу поддержки этой ПС. Вполне возможно, что после этого кошелек мошенника будет заблокирован. Кроме того, в службе поддержки можно выяснить паспортные данные владельца кошелька, незаконно получившего деньги. Знание этих данных позволит обратиться в суд с иском об истребовании денежных средств.

На мошеннический сайт можно пожаловаться на специальных сервисах, предназначенных для блокирования вредоносных сайтов.

Кроме того, подать жалобу на компьютерное мошенничество можно на сайте Роскомнадзора (это орган по надзору в сфере информационных технологий).

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ПОРТАТИВНЫХ УСТРОЙСТВ?

Сегодня почти каждый житель нашей страны имеет два обязательных атрибута эпохи: банковскую карту и смартфон. Все больше клиентов банков устанавливают в свои телефоны программы электронного банкинга. Хотя это удобно и практично, в тоже время небезопасно.

Дело в мобильном вирусе – маленькой программке, которую изобрели мошенники. Эта программа лежит в вашем смартфоне – вы о ее наличии даже не знаете. Между тем с ее помощью злодеи имеют доступ ко всей информации в вашем телефоне. В первую очередь к банковским картам. Мобильный вредонос втайне от вас может перевести часть денег с вашей карты на подконтрольный мошенникам счет или приобрести товар для злоумышленника за ваши деньги.

Кто-то подумает, что это напрасные страхи, ведь каждая операция с вашей картой требует код подтверждения. А код этот мы получаем с помощью СМС от банка. Но мобильные вирусы давно научились перехватывать эти сообщения и переправлять их мошенникам, которые нас обчищают. В итоге жертва мошенника, потерявшая миллион рублей, приходит в гневе в банк и узнает, что с банковской карты было сделано 10 финансовых операций – и все они подтверждались с привязанного к карте телефона.

Мошенники ежедневно заражают сотни устройств по всему миру. Их задача поразить как можно большее количество смартфонов, при этом действовать они могут через год или два. Они могут отправить вирус на телефон, где нет мобильного банка, и вирус будет ждать того часа, когда вы его подключите. После этого он отправит соответствующее сообщение хакерам. И они начнут с вами «работать».

Наши мобильные давно уже представляют собой компьютеры, управляемые операционной системой, которую легко взломать. Кстати, что интересно, почти все электронные черви, засылаемые на наши телефоны, предназначены для системы «Андроид».

То, что эти трояны в основном нацелены на «Андроид», обусловлено тем, что эта операционная система стоит в 80% всех смартфонов в мире. А разработка вредо-

носной программы стоит довольно дорого. Так что это вопрос рентабельности. Мошенники регулярно придумывают все новые вредоносные программы.

Как защититься?

Конечно, стопроцентной защиты в наше время не дает ничто. Но соблюдение простых правил безопасности поможет вам избежать потери денег.

1. Купите простой телефон без операционной системы и привяжите к нему ваш мобильный банк.

Помните старые добрые телефоны, с которых в начале 2000-х мы звонили, писали СМС и на которых играли в «змейку» и тетрис? Не пожалейте 500 рублей – купите себе эту простую трубку, на нее никакой вредонос не установится. И к этому номеру подключите вашу карту или банковский счет. Пусть все СМС с подтверждениями и о денежных операциях приходят на этот мобильник. Такой способ почти полностью обезопасит вас.

2. Внимательно читайте, к каким функциям вашего телефона требует доступ приложение, которое вы хотите скачать.

Если видите, что, к примеру, «живые обои» или любое другое украшение для рабочего стола просят дать доступ к внутренней памяти, отправке СМС или страницам в социальной сети, стоит как минимум задуматься. С чего бы это вы должны давать конфиденциальную информацию о себе приложению, которому все это для работы не требуется?

3. Обязательно устанавливайте антивирус.

Борцы с компьютерными мошенниками удивляются странной безответственности наших граждан. Если на компьютер или ноутбук все мы ставим антивирус в обязательном порядке, то на смартфонах почему-то этого не делаем. Экономим память смартфона. Предпочитаем вместо

защитной программы закинуть в телефон побольше музыки или игр. Между тем сегодня стандартные антивирусы пресекают почти все мобильные вирусы, которые выпускались за последние пять лет.

Как вредоносное ПО попадает на портативные устройства

I. Вместе с приложениями

В большинстве случаев вирусы попадают на устройство под видом каких-то безобидных приложений: браузеров, плееров, игр, книг, и даже антивирусов. Причем это может быть приложение, которое только «притворяется» оригинальным, а на самом деле имеет абсолютно другое содержание, либо оригинальное приложение, но с одним маленьким отличием – добавленным зловредным кодом. Получить такой «сюрприз» можно в том случае, если загружать приложения не из Play Маркет, а с каких-то сторонних сайтов или форумов.

Один из самых распространенных сценариев получения вредоносного приложения выглядит так: на каком-либо сайте появляется окно с требованием обновить какую-то программу, потому что установленная на устройстве якобы устарела и больше не поддерживается, или появляется сообщение о том, что устройство заражено вирусами и его надо срочно проверить. На самом деле этой программы может даже не быть на вашем устройстве, а такое сообщение показывается абсолютно всем пользователям, заходящим на данный сайт, даже если у них самая последняя версия якобы не обновленного приложения.

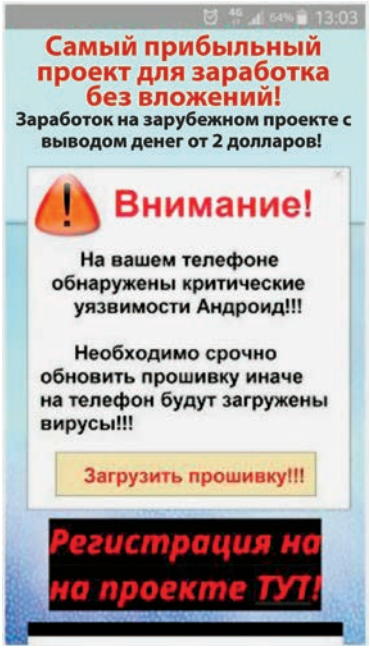


Рис. 1. Пример баннера, который сообщает о якобы обнаруженных уязвимостях.

Когда пользователь соглашается с обновлением, проверкой или просто открывает подобный сайт, на его устройство загружается установочный файл вирусного приложения (с расширением .apk), которое имеет различные вредоносные разрешения (это действия, которые может выполнять приложение на устройстве после установки), например, разрешение отправки SMS на короткие номера.

После установки приложение активируется и начинает действовать, в случае с примером выше – начинает отправлять SMS на короткие номера незаметно для пользователя. В итоге, баланс SIM-карты быстро уменьшается до минимально возможного значения. Конечно, сценарии

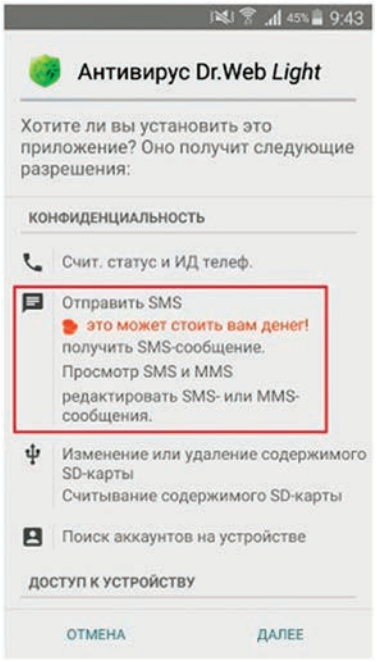


Рис. 2. Попробуем установить подделку одного из самых известных антивирусов – Dr. Web. Обратите внимание на разрешения

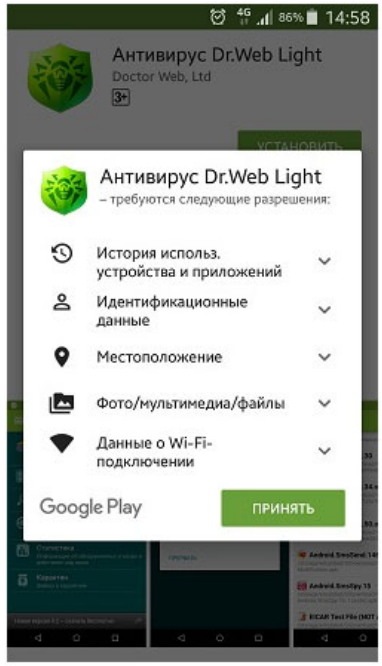


Рис. 3. А вот разрешения оригинального приложения

могут отличаться, например, вам могут прислать вредоносную ссылку по SMS или E-mail, но в целом, 99% устро, йств заражаются именно через установку какого-то приложения.

Итак, основные правила мобильной безопасности и подробные объяснения о каждом из них:

1. *Никогда и ни при каких условиях не устанавливайте приложения с каких-либо источников, кроме Play Маркет. Если после посещения какого-то сайта вы видите загрузившийся файл с расширением .apk, например, flash_player.apk, лучшим решением будет его немедленное удаление (загруженные файлы хранятся в Мои файлы – Downloads).*

   Однако необходимо понимать, что полностью безопасной системы в мире не существует, и в Play Маркет также могут проникнуть вредоносные приложения, правда их количество в десятки раз меньше и пробиться туда им гораздо сложнее.
2. *Не переходите по неизвестным ссылкам, особенно по тем, которые вы получили по SMS, MMS или e-mail от неизвестных отправителей.*

   Чего только не пишут злоумышленники, чтобы заставить вас нажать на заветную ссылку: обещают гарантированные миллионные выигрыши в лотерею, предлагают купить какие-то товары со скидкой 95%, или сообщают о 1334 женщинах, которые находятся в 300 метрах от вас и хотят познакомиться только с вами. В основном вирусы изобилуют на сайтах, которые предлагают что-то получить или скачать бесплатно, сайтах для взрослых, сайтах, предлагающих зарабатывать по 1000 долларов в интернете, ничего не делая, и т.д.

   Также такие сообщения могут приходить и от ваших знакомых, мошенники научились подделывать номера.

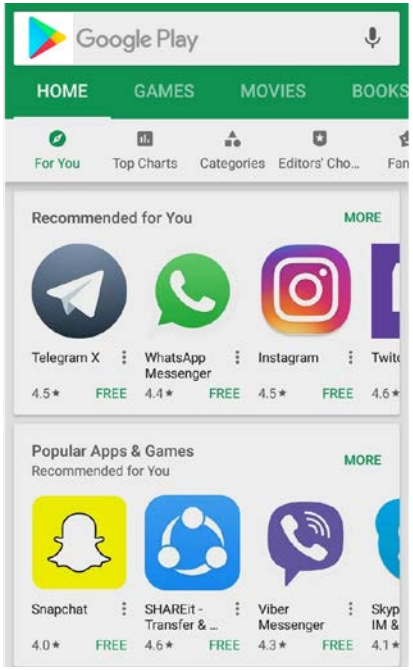


Рис. 4. Рекомендуется загружать приложения только из Google Play Маркет

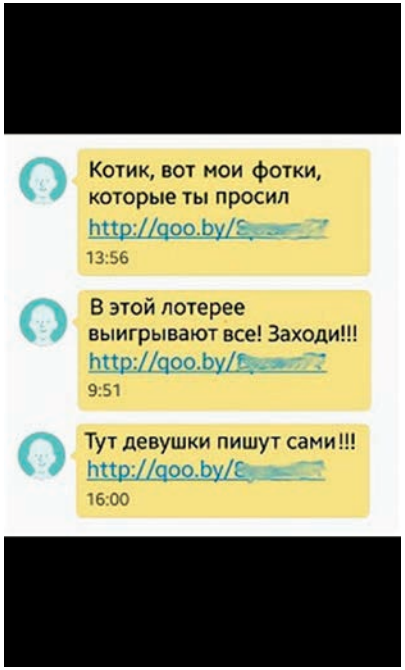


Рис. 5. Образцы сообщений от мошенников, присланные по SMS

3. *Отключите услугу MMS у оператора связи или хотя бы автополучение MMS на вашем устройстве.*
4. *Не подключайте банковскую услугу «Автоплатеж» (автоматическое пополнение счета мобильного телефона при снижении суммы на нем до какого-то значения).* Если вдруг на ваше устройство установится вредоносное приложение, которое может отправлять SMS на короткие номера, то с помощью данной услуги баланс будет постоянно пополняться до тех пор, пока средства на карте не закончатся. SMS от банка при этом блокируются.

Как понять, что на смартфоне или планшете с Android появился вирус?

К сожалению, не существует каких-то однозначных признаков заражения вредоносным ПО, т.к. все зависит от того, какой вирус вам попался. Присутствие некоторых замечаешь сразу после установки (например, появляется какой-то баннер и блокируется доступ к устройству), другие могут долгое время находиться на устройстве и ничем себя не выдавать. Тем не менее, в большинстве случаев признаки такие:

- Неожиданно быстро начинает садиться батарея,
- Появляются большие счета за мобильную связь,
- Большой расход интернет-трафика непонятными приложениями,
- Появление незнакомых программ,
- Устройство начинает сильно тормозить.

II. «Фейковые» точки доступа

Использование общественных точек доступа Wi-Fi также может привести к потере личных данных и заражению устройств. Опасность кроется в «фейковых» точках доступа, которые успешно маскируются под известные сети.

Как мошенники создают подставные точки доступа?

Мошенники в качестве одного из способов часто пользуются невнимательностью пользователей и создают «клоны» или похожие на общественные точки Wi-Fi. Свою вредоносную точку хакеры размещают в непосредственной близости от легитимной точки доступа. В качестве поддельных имен злоумышленники могут использовать следующие трюки:

- название и/или модель роутера: DIR-300, ASUS;
- популярные названия бесплатных Wi-Fi, к примеру, MosMetro_Free, Beeline_Free_Wi-Fi, но с незначительными изменениями в имени;
- точки доступа заведений и зданий, которые могут быть защищены паролем, к примеру, McDonalds_WiFi_Free или название аэропорта;
- точки доступа с забавными названиями, рассчитывая на любопытство владельцев гаджетов: h0lyava, MaminHackir, blondinka.

«Отличить» фейковую точку доступа проще всего, узнав название легитимной – у официанта или прочитав название в меню или на информационном стенде. В остальном же разобраться практически нереально.

В каких местах хакеры могут атаковать обычных пользователей?

Наиболее опасными с этой точки зрения могут быть общественные места, в которых люди часто прибегают к помощи бесплатного Wi-Fi. При этом атаки могут быть организованы по нескольким причинам: злоумышленники желают завладеть конкретной конфиденциальной информацией, целенаправленно заражают устройства, внедряя вредоносы, а также используют аналог публичной точки для пропаганды.

Как уберечь свое устройство от нападений мошенников по Wi-Fi?

Самый верный способ отгородиться от возможных атак, особенно если в устройстве хранится очень важный информация, не включать без надобности Wi-Fi и не подключаться к бесплатным сетям в общественных местах, особенно популярных.

Кроме того, будет полезным включить «подтверждение подключения» к сетям, которые считаются известными и не вызывают опасений. Если же подключение к публичной точке жизненно необходимо, рекомендуем не использовать банковские клиенты и другие программы, напрямую связанные с денежными счетами, в открытых сетях.

И напоследок еще один совет для тех, кто все же стал жертвой мобильного вредоноса. Если вы вдруг сейчас запросили баланс и поняли, что вас обчистили, не нужно бежать в ближайший отдел полиции и объяснять проблему. При всем уважении к полицейским, нужно понимать: им довольно сложно понять все тонкости кибермошенничества и того, как у вас украли деньги с помощью мобильного вредоноса. В итоге, прежде чем ваше дело попадет в нужный отдел, пройдут драгоценные дни и недели, а может, и месяцы. Рекомендуем обращаться с заявкой через специальную форму на сайте https://mvd.ru/. В заявлении следует указать обстоятельства, при которых вы стали жертвой заражения, кражи или ограбления, а также такие данные о телефоне, такие как производитель и модель устройства.

Ваша заявка быстро попадает в нужный отдел. Не исключено, что вы стали жертвой целой мошеннической сети, которую как раз отслеживают агенты полиции. Чем быстрее ваша заявка через Интернет поступит в отдел, тем больше шансов на счастливый исход вашей истории.

ПРЕИМУЩЕСТВА ПЛАСТИКОВЫХ КАРТ

Существует много признаков, по которым можно классифицировать банковские карты, мы приведем наиболее значимые из них.

По типу финансовых средств: «дебет-кредит»

По типу средств, размещенных на карте, выделяют дебетовые и кредитные карты. В России существует некоторая путаница в использовании термина «кредитная карта». Иногда им обозначают любые пластиковые карты, иногда – только карты с кредитными средствами. Причина этой путаницы в том, что исторически первые пластиковые карты были именно кредитными, а не дебетовыми. Поэтому за всеми картами сохранилось название «кредитных».

- Дебетовые

На дебетовой пластиковой карте хранятся исключительно личные денежные средства держателя. Оплата товаров и услуг, а также снятие наличных возможны только при наличии средств на счете, привязанном к данной карте. Помимо этого, существуют овердрафтные карты, позволяющие производить платежи как за счет средств держателя карты, так и за счет кредита, предоставляемого банком в случае недостатка средств на счете. Дебетовые карты, которые оформляются предприятием для своих работников в целях перечисления зарплаты и других начислений, называются «зарплатными». Такие карты выдаются в рамках «зарплатного проекта», то есть договора, заключенного между банком и предприятием. Зарплатные пластиковые карты являются дебетовыми, иногда – овердрафтными.

- Кредитные

На кредитной карте, как было упомянуто выше, хранятся деньги, которые банк предоставляет в пользование держателю карты. Каждый банк устанавливает определенный кредитный лимит, в рамках которого клиент может совершать покупки и снимать наличные. При этом на кредитной карте могут храниться и собственные средства держателя. Кредитные карты различаются по схеме начисления процентов за пользование кредитом. Большинство кредитных пластиковых карт имеется так называемый грейс-период, или льготный беспроцентный период, в течение которого на использованные средства не начисляются проценты (обычно 50–60 дней), если задолженность будет погашена в течение этого срока. Существуют также кредитные карты, в которых проценты начисляются сразу после совершения покупки, то есть по ним отсутствует льготный беспроцентный период.

По категориям карты: от классики до «платины»

Чем выше категория карты, тем больше у нее возможностей, но и стоимость ее обслуживания возрастает пропорционально. Существуют карты классической категории, золотой, платиновой и более высокие «черные» карты, как например, MasterCard Black Edition или Visa Black. Кроме того, обладание золотой, платиновой или тем более «черной» картой подчеркивают статус ее держателя, что для многих немаловажно. С повышением категории карты растут кредитные лимиты.

Следует также отметить, что чем выше статус карты, тем больше привилегий она предоставляет держателю. Так, международные платежные системы предоставляют скидки для держателей премиальных карт, а банки предусматривают особый сервис в виде приоритета обслуживания, консьерж-службы и многого другого, что зависит от конкретного банка-эмитента. Существует также категория виртуальных, карт: они не имеют физического носителя и предназначены исключительно для совершения покупок через Интернет, без возможности снятия наличных.

По типам дополнительных сервисов: большие возможности

Кобрендинговые пластиковые карты выпускаются в партнерстве с различными крупными фирмами, как правило, сетями. Такие карты предоставляют их держателю какие-либо привилегии или бонусы от компании-партнера банка. Например, если партнером выступает авиакомпания или сервис продажи авиабилетов, то при совершении покупок клиент получает так называемые бонусные «мили», которые затем можно потратить на покупку авиабилета. Кобрендинговую карту имеет смысл выбирать только в том случае, если вы уже являетесь активным пользователем услуг компании-партнера. Во всем остальном подобные карты ничем не отличаются от других пластиковых карт.

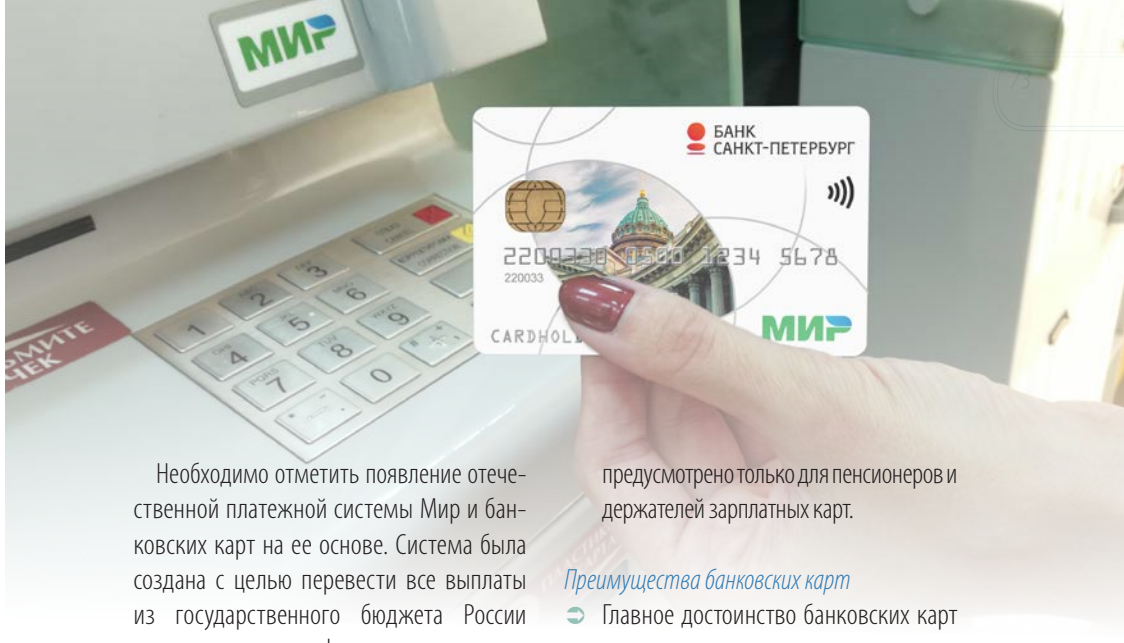
Еще одна привлекательная услуга, которую предоставляют некоторые банки в дополнение к пластиковой карте – это Cash Back. Смысл опции в том, что, совершая различные покупки по кредитной или дебетовой карте клиент получает определенный процент от всей потраченной по карте сумме обратно на свой счет. Например, если Cash Back 3%, и вы за месяц совершили операций по карте на 100 000 руб., то банк вернет на нее до 3000 руб.

Что следует учитывать, выбирая карту

К наиболее востребованным и популярным банковским продуктам сегодня относятся платежные карты системы Visa. Тем не менее, терминальные системы готовы принимать платежные инструменты обоих систем. Если рассматривать данные продукты с точки зрения валютных отношений, то карты от системы Visa, которая является американской системой, как правило, ориентируются на доллар.

Что же касается пластиковых карт Mastercard, то их принцип функционирования сосредоточен на евро. Связано это с тем, что данная платежная система приспосабливалась в первую очередь к странам Европы. Безусловно, пластиковые карты и той и другой системы практически не уступают друг другу и широко используются во всем мире, однако в целях экономии своего капитала держателям карт при выборе платежной системы следует исходить из конкретной страны, где клиент будет производить платежные и расчетные операции.

Конвертация визовых карт осуществляется по курсу валюты США, то есть по доллару. Если допустить, что человек поехал в путешествие в какую-либо европейскую страну с картой Visa, то при осуществлении какой-либо платежной операции средства на его карточном балансе сперва будут переведены в доллары, и лишь потом в евро. Конвертация проходит в два этапа, что удорожает денежную операцию. Такие затраты исключаются у карты системы Mastercard, так как и евро, и доллар выступают в данной системе как основные валюты.



Необходимо отметить появление отечественной платежной системы Мир и банковских карт на ее основе. Система была создана с целью перевести все выплаты из государственного бюджета России и государственных фондов на независимую платежную систему, контролируемую РФ. Это позволит оградить граждан от рисков отключения (запрета) иностранных платежных систем в России, таких как Visa и MasterCard в России. Однако, на текущий момент, карта имеет ряд существенных недостатков:

- можно использовать для оплаты товаров и услуг, а также снятия наличных в банкомате, только на территории России и Армении;
- ограниченное распространение как в простых, так и сетевых магазинах. Например, карту принимают к оплате только в одном крупнейшем зарубежном интернет магазине в мире Aliexpress;
- тарифы на ежегодное обслуживание банки устанавливают самостоятельно, в связи с чем некоторые банки могут устанавливать завышенные тарифы на ее обслуживание. Бесплатное обслуживание предусмотрено только для пенсионеров и держателей зарплатных карт.

Преимущества банковских карт

- Главное достоинство банковских карт заключается в их универсальности. В наше время пользователи любой финансовой системы могут пользоваться картами как в своей родной стране, так и в любой зарубежной. Это обусловлено тем, что почти все финансовые системы уже давно перешли на международный уровень.
- Еще одно важное преимущество заключается в том, что при перевозе карты через границу с крупными денежными накоплениями они не вносятся в декларацию в отличие от наличных, поэтому с пластиковой картой никогда не возникнет проблем на границе.
- Существенное преимущество «пластика» – удобство. Имея свою карту, человеку не приходится носить с собой наличные. Карта позволяет клиенту в любой момент воспользоваться своим счетом, например, расплачиваясь за покупку в супермаркете.

- Благодаря возможности оформления таких карт через интернет сегодня можно существенно сэкономить время.
- Стоит помнить, что оставшаяся на счету сумма может постоянно увеличивается за счет накопительного процента.
- Потеряв кошелек с наличными, вы вряд ли сможете его вернуть. Что касается карточки, то нашедший человек не сможет ее обналичить. Как только владелец карты заметит, что его карта утеряна, он может сразу же осуществить ее блокировку, приостановив все операции по ней с помощью звонка в банк. Восстановить карту достаточно легко. Все, что от вас потребуется – обратиться в ближайшее отделение банка, где вам придется составить заявление, и уже через 2-3 дня карта вновь будет у вас на руках с вашими накоплениями. Именно безопасность является самым главным преимуществом пластиковых карт.
- Пластиковые карты являются достаточно защищенным платежным инструментом. От ошибки кассира или собственной невнимательности во время покупок можно уберечься, если проверять подлежащие списанию суммы. Можно перестраховаться при использовании карты и при совершении покупок в интернет магазинах. Обо всех операциях по счету, привязанному к карте, можно узнать, запросив выписку и с помощью информирования посредством смс.

Следует знать, что несмотря на высокую степень защищенности карточки все же подвержены различным атакам скраббе-ров и хакеров. Мошенники, занимающиеся взломом карт, могут отследить банковские операции и подобрать к ним пароль.

Недостатки банковских карт

- Из минусов использования карт можно сразу назвать малую плотность банкоматов и недостаточную инфраструктуру за пределами крупных городов. В небольших городах не все торговые точки работают с картами. С проблемами оплаты кредиткой в кафе или в магазине в небольших населенных пунктах сталкивались практически все владельцы карт.
- К тому же карты полностью «прозрачны» для спецслужб, которые могут отследить все операции.

Какую банковскую карту выбрать?

Начнем с вопроса, в каких случаях в дополнение к дебетовой пластикой карте необходимо иметь еще и кредитную? В принципе, наличие «запасной» карты с кредитными средствами актуально всегда – в дальних поездках, при необходимости совершения срочных платежей или покупок, или просто при возникновении проблем с дебетовой картой кредитка может стать настоящей «палочкой-выручалочкой».

На сегодняшний день кредитная пластиковая карта является крайне удобным и полезным средством для совершения платежей. Кредитная карта не подходит только для снятия наличных (за снятие наличных банк взимает относительно высокую комиссию). При желании можно найти кредитную карту с бесплатным обслуживанием (банки часто устраивают такие акции) и продолжительным грейс-периодом, то есть периодом, в течение которого можно пользоваться картой и не платить проценты, что делает ее особенно выгодной.

Виртуальная карта актуальна только для тех, кто совершает множество покупок через Интернет или ведет в нем свою профессиональную деятельность. Она необхо-

дима в том случае, если хотите обезопасить свою дебетовую карту от мошенничества и кражи личной информации, что иногда случается при покупках в Интернете. В этом случае перед совершением операции необходимо перевести необходимую сумму с дебетовой карты на виртуальную.

Однако нужно помнить о том, что снятие наличных с виртуальной карты невозможно, так же, как и оплата в офлайн-магазинах. Дебетовая карта является универсальным инструментом: если вам необходима пластиковая карта исключительно для пользования собственными средствами, то дебетовой карты будет достаточно. Она также является наиболее удобной с точки зрения снятия наличных.

По материалам статьи: https://www.kp.ru/guide/plastikovye-karty-bankov.html

КАРТА ИЛИ НАЛИЧНЫЕ: КАКИЕ СПОСОБЫ ОПЛАТЫ ВЫГОДНЕЕ ИСПОЛЬЗОВАТЬ ЗА ГРАНИЦЕЙ?

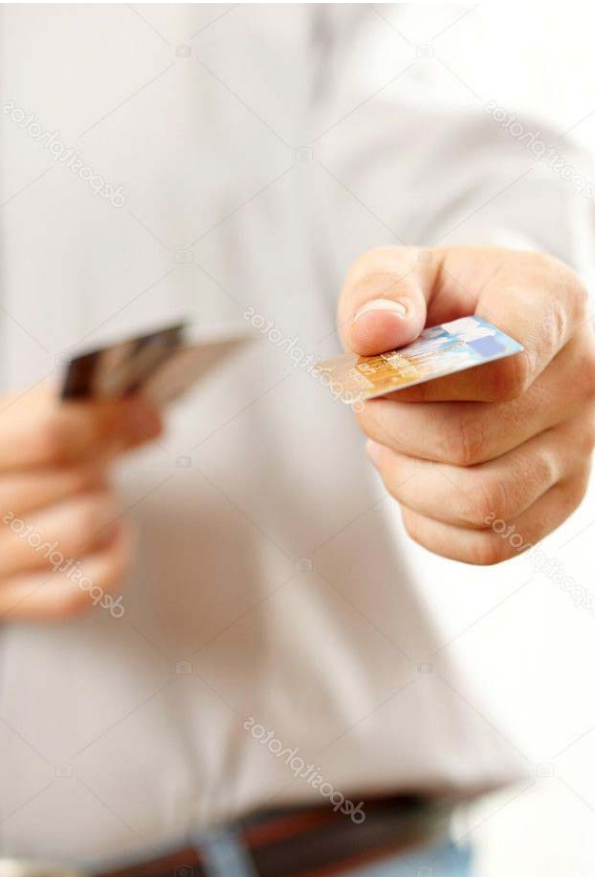
Эксперты настоятельно рекомендуют в зарубежных поездках пользоваться банковскими картами, так как этот способ хранения денег считается наиболее безопасным. «Пластиком» удобно платить за товары и услуги, вы не рискуете потерять наличность. Сегодня не имеет значения, какая у вас карта – американская Visa или международная MasterCard. Имеет значение, какой счет привязан к карте. Лучше, если это будет счет в долларах или евро.

Допустим, вы приобрели в Милане парфюм, расплатившись картой Visa российского банка с рублевым счетом. В этом случае рубли конвертируются в европейскую валюту согласно курсу платежной системы. Банк также может снять с вас проценты (от 1 до 5) за совершение операции по рублевой карте за границей. Если бы карта была в евро, вам удалось бы избежать конвертации и комиссии – вы просто оплатили бы покупку в евро, так же, как в России вы оплачиваете покупки в рублях.

Отправляясь в страны, где в ходу отличная от доллара или евро валюта, имейте в виду, что возможна и двойная конвертация. Так, если вы расплатились в датском магазине картой системы MasterCard и банк использует для расчетов с платежной системой рубли, система переведет их в датские кроны по своему курсу. Если же расчеты осуществляются в долларах, система конвертирует датские кроны в доллары, а ваш банк переведет их в рубли по собственному

курсу. В подобных случаях рублевая карта более выгодна.

В некоторых иностранных торговых точках у вас могут уточнить, какой валютой вы желаете расплатиться: местной, долларами или евро либо же рублями. В таких случаях смело выбирайте местную валюту. Оплатив рублями, вы рискуете потерять в деньгах из-за комиссии от банка магазина и тройной конвертации (если валюта карты и расчетов не совпадают). Поэтому, отправляясь, например, в Китай, имейте в виду, что даже держателям долларовых карт там рекомендуют выбирать расчеты в юанях. Одна валюта будет переведена в другую, но тройной конвертации не произойдет.



Несмотря на все преимущества карты, полностью заменить ею наличные деньги не получится. Осталось еще немало мест, где карты просто не принимают, а где-то расчеты наличными более уместны.

Находясь за рубежом, вы можете свободно снимать с вашей рублевой карты как доллары и евро, так и местную валюту через банкомат. Принцип здесь тот же, что и при расчетах в торговой точке: одна валюта конвертируется в другую, но дополнительно банк может начислить свою комиссию за снятие наличных. Поэтому некоторым количеством мелких денег следует запастись еще до выезда за рубеж. Это можно сделать в банке или обменном пункте. Банк также может устанавливать ограничение на сумму средств, снимаемых за один раз.

Следует заметить, что не во всех зарубежных банках вы сможете найти привычные для нас обменные кассы. Тогда придется общаться с сотрудником банка, что может быть осложнено языковым барьером. Обменные пункты, как правило, предлагают лучший курс, чем банки, но здесь вы можете обнаружить некоторые подводные камни. Указанный на вывеске курс, вероятнее всего, будет действителен только при покупке достаточно большой суммы валюты. Но об этом не всегда предупреждают – велика вероятность, что вам просто обменяют деньги по менее выгодному курсу или просто обсчитают. В обменных пунктах также часто действуют различные комиссии, к тому же есть риск получить испорченные или фальшивые купюры.

Рекомендовано при планировании поездки в какую-либо страну заранее узнать о том, какие валютные ограничения там действуют. Так, в некоторых странах на обмен долларов действует определенная комиссия. Например, на Кубе ее размер равен 10% от обмениваемой суммы. Разумеется, в такие страны лучше отправляться с евро. Если же в ваших планах посетить некий отдаленный остров или другую малонаселенную местность, возьмите с собой достаточное количество местной валюты. Ведь велика вероятность не встретить там ни одного банка или даже банкомата.

Где иметь при себе наличные необходимо:

- в Греции, особенно в островной ее части; в Германии и других консервативных странах, где не торопятся переходить на безналичную оплату;
- в странах с собственными платежными системами, такими как в Японии;
- в странах с развитой уличной торговлей, например, в Юго-Восточной и Средней Азии;
- в Камбодже и других странах, где в ходу доллары – там вам не придется обменивать деньги на местную валюту.

https://www.exocur.ru/karta-ili-nalichnyie-kakie-sposobyi-oplatyi-vyigodnee-ispolzovat-za-granitsey/

КАК ОТЛИЧИТЬ ФАЛЬШИВЫЕ ДЕНЬГИ ОТ НАСТОЯЩИХ

Если какая-либо рублевая, долларовая или евро купюра вызвала у вас сомнение в своей подлинности, то «опознание» лучше всего проводить, вооружившись небольшим увеличительным стеклом (4–8 крат). При этом наиболее просто выявить подделку, если рядом с сомнительной купюрой положить настоящую и внимательно сравнить их.

Для быстрого и достоверного определения подлинности купюры без использования специальных приборов посмотрите купюру на просвет и убедитесь в наличии водяного знака, а также защитной полосы. Если какие-либо отдельные из этих деталей (или все) отсутствуют – вероятность, что купюра фальшивая приближается к 100%.

Кроме того, убедитесь в наличии защитных волосков в бумаге купюры, проверьте, не дорисованы ли они на банкноте.

Рассмотрите купюру с лицевой и оборотной стороны и убедитесь, что на купюре нет расплывов краски, изображения четкие, линии сплошные (не состоят из точек), нет глянцевого блеска купюры.

Буквы и цифры серийного номера должны быть расположены строго на одной линии, расстояния между цифрами одинаковые. Размер всех знаков номера – одинаковый. Одноименные знаки в номерах имеют одинаковое начертание. На фальшивках же буквы и цифры в серийных номерах часто «прыгают».

Рассмотрите серийный номер купюры и микропечать. Серийный номер должен иметь характерные признаки высокой печати, а микропечать должна читаться. Это наиболее верные признаки подлинной купюры, позволяющие отличить ее даже от очень хороших подделок.

Наиболее подделываемые российские деньги – это тысячерублевые купюры, которые в последнее время научились подделывать наиболее профессионально. Тем не менее, определить фальшивую банкноту можно и без специальных приборов.

Обратите внимание на 8 основных признаков:

1. Водяной знак. Для фальшивомонетчиков его имитация – давно уже не проблема, но у них, по сравнению с Госзнаком, работа все-таки топорная. На подлинном «Билете Банка России» распределение тонов неравномерное: одни участки темнее, другие светлее. На фальшивках водяной знак однотонный и темнее, чем на настоящих купюрах.
2. Герб Ярославля с изображением медведя. Если купюру немного наклонить, то герб меняет цвет с малинового на зеленый.
3. Микроперфорация в виде вертикальной цифры «1000» под гербом и слегка заходящая на герб (такая же микроперфорация есть и на 5-тысячных купюрах). Ее жулики делают или иголками, или на специальных машинках, поэтому на обратной стороне остаются

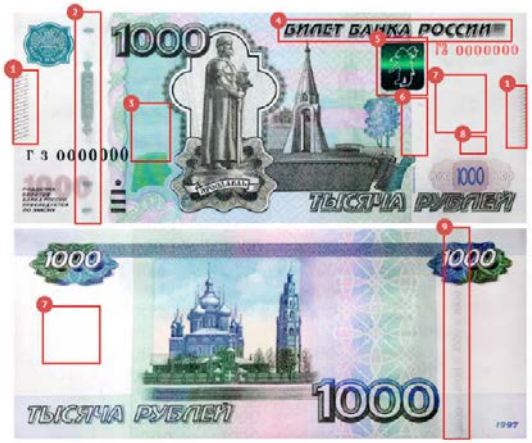
ПОДЛИННОСТЬ БАНКНОТ ОПРЕДЕЛЯЕТСЯ:

- на просвет
- при изменении угла зрения
- с помощью лупы
- наощупь
- датчиками магнитного поля
- ультрафиолетовыми и инфракрасными датчиками
- оптическими датчиками

шероховатости. Достаточно провести пальцем, чтобы эту шероховатость почувствовать. У подлинной банкноты дырочки ровные и на ощупь без шероховатостей.

4. Увеличенный рельеф надписи «БИЛЕТ БАНКА РОССИИ». Рельефность надписи легко воспринимается на ощупь.
5. Металлизированная защитная нить. Её фальшивомонетчики так же научились подделывать, но до аккуратности Госзнака не дотягивают.

6. Вертикальная орнаментная полоса. Орнаментные полосы расположены как на лицевой, так и оборотной сторонах купюры. Если денежку рассматривать на просвет, то будут видны не окрашенные элементы.
7. Метка для людей с ослабленным зрением на лицевой стороне купюры. Метка в виде трех полосок с точкой вверху обладает повышенной рельефностью.
8. Защитные волокна. Еще на стадии изготовления в «денежную» бумагу внедряются защитные волокна желто-красного, красного и светло-зеленого цветов.



1000 рублей
(модификация 2010 г.)

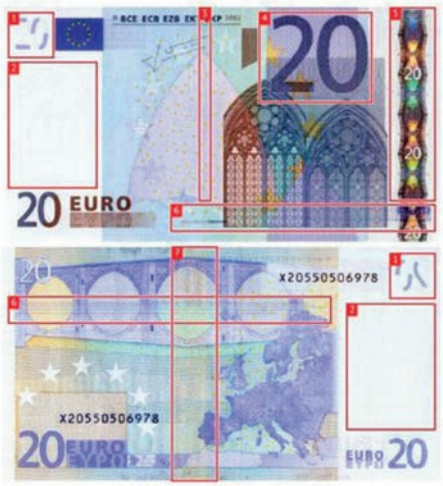
1. На полях имеются тонкие косые штрихи
2. При наклоне купюры на защитной линии появляется либо изображения чисел «1000», либо радужный блеск
3. Полосы меняют цвет при наклоне
4. Текст «Билет банка России» рельефен
5. Полоса на гербе Ярославля перемещается при наклоне
6. При просвете под гербом видно число «1000» из микроотверстий
7. При просвете виден портрет Ярослава Мудрого
8. Рядом с портретом находится водяной знак «1000»
9. При просвете повторяющиеся числа «1000» выглядят светлыми на тёмном фоне

5000 рублей

1. Защитная нить серого цвета
2. Цифры «5000» на защитной ленте, которые смещаются при наклоне купюры
3. Магнитные и люминисцентные элементы
4. Изображение берега Амура из мелких графических элементов
5. Яркая полоса на гербе Хабаровска, которая перемещается при наклоне купюры
6. Число «5000» из микроотверстий
7. Водяные знаки: портрет Муравьёва-Амурского и число «5000»
8. Рельефные надписи «Билет банка России», «5000», «Пять тысяч рублей» и метка для слабовидящих людей
9. 7 полос микротекста «ЦБРФ5000»

100 долларов
(модификация 2013 г.)

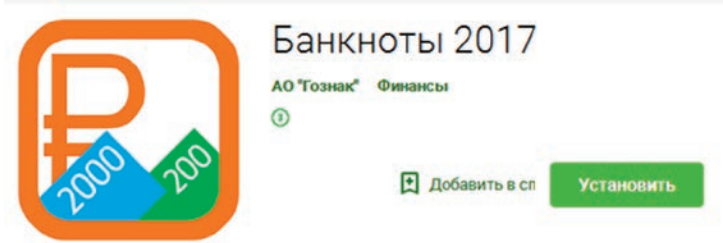
1. Подписи экс-министра финансов и казначея США
2. На воротнике Франклина написано «United State of America»
3. При наклоне купюры на тр ,хмерной защитной ленте появляются либо колокольчики, либо числа «100»
4. На чернильнице при наклоне появляется зел ,ный колокольчик
5. Цитаты из Декларации Независимости США
6. Число «100» меняет цвет при наклоне купюры
7. Виньетка с изображением южного фасада Индепенденс-Холла
8. На часах колокольни выставлено время – 10:30
9. Число «100» большого размера и золотого цвета с градиентом



20 евро

1. Цифра, обозначающая номинал купюры, видна полностью только на просвет. При обычном просмотре видны только части цифры
2. Водяной знак, видимый только на просвет, состоит из двух частей: изображение главного элемента купюры, то есть картинки, и номинала
3. Невидимая защитная нить на поверхности с указанием номинала купюры
4. Рельефный номинал купюры, его легко можно почувствовать кончиками пальцев
5. Синеграмма в виде полосы, состоящей из повторяющихся надписей «euro» и номинала купюры
6. Микротекст в виде повторяющегося слова «евро» на латинском и греческом языках, составляет линию, которая тянется через всю банкноту
7. Вертикальная линия, образованная повторяющимися изображениями логотипа евро и номинала, хорошо видна только под определенным углом зрения

В АО «Гознак» разработали мобильное приложение «Банкноты 2017» предназначеное для распознавания банкнот номиналом в 200 и 2000 рублей, выпущенных в обращение Банком России. Приложение позволяет сканировать визуальный образ банкноты при помощи камеры смартфона, анализирует изображение для определения номинала представленной банкноты, демонстрирует дополнительную анимацию символов городов, изображенных на банкнотах, с использованием технологии дополненной реальности, оценивает наличие и расположение на банкноте некоторых публичных признаков подлинности.



ПЕНСИОННОЕ И СОЦИАЛЬНОЕ ОБЕСПЕЧЕНИЕ