ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНТЕРНЕТ

Васев Ю. В.

Актуальность ИБ

Перевод большинства информационных архивов, денежных средств и коммуникаций в электронную форму создал самостоятельный тип актива – информацию. Как любая ценность, она подвергается посягательствам со стороны различных мошенников. Возникают существенные риски и в области обеспечения государственной безопасности в сфере информации, основные угрозы названы в Доктрине государственной информационной безопасности. Игнорирование возникающих проблем приводит к потере конкурентоспособности как на государственном, так и на корпоративном уровне. Страдают от преступлений, совершаемых в информационной сфере, и граждане.

Безопасное поведение в сети **ИНТЕРНЕТ**

Правила минимизируют риски пострадать от любого вида мошенничества

Васев Ю. В.

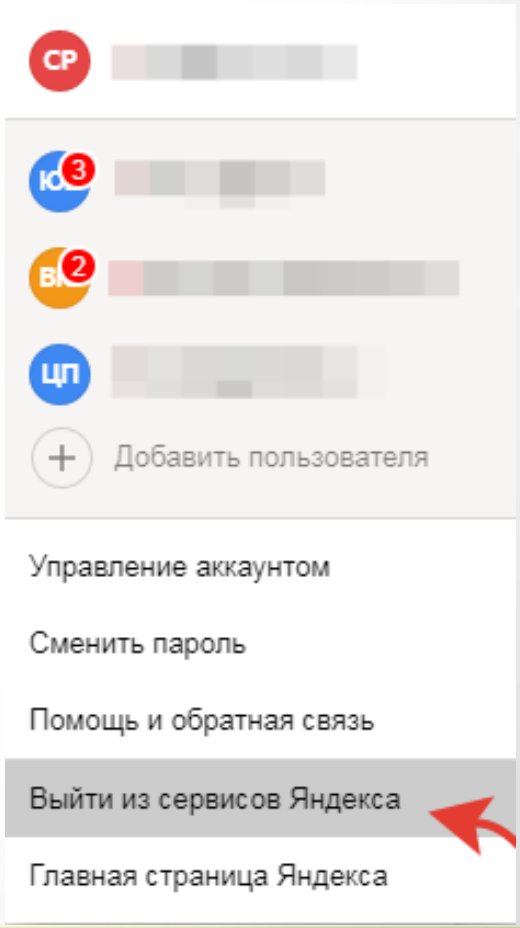
Конфиденциальная информация

Конфиденциальная информация — информация, являющаяся *конфиденциальной*, то есть «доверительной, не подлежащей огласке, секретной»; это понятие равнозначно с понятиями тайны или секрета.

Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.

«Выход» из любых сервисов

Выполняя вход в электронную почту, или социальную сеть с чужого устройства (планшет, ноутбук, настольный ПК), после работы не забывайте «разлогиниться», то есть выйти из своего аккаунта.



Отключение WI FI

Специалисты по компьютерной безопасности обнаружили уязвимость протоколов шифрования WPA2, которые используются в сетях Wi-Fi по всему миру. Используя систему **Key Reinstallation Attacks (Kracks)** можно получить доступ даже к зашифрованной информации, если устройство подключено к Wi-Fi.

Уязвимости подвержены все устройства с функцией Wi-Fi, особенно агрессивно взлом может действовать на 40% гаджетов на платформе **Android**. **Kracks** несет угрозу вне зависимости от выбора оператора связи и может похитить любые данные: фото, переписку, историю посещений сайтов.

Использование WI FI в кафе

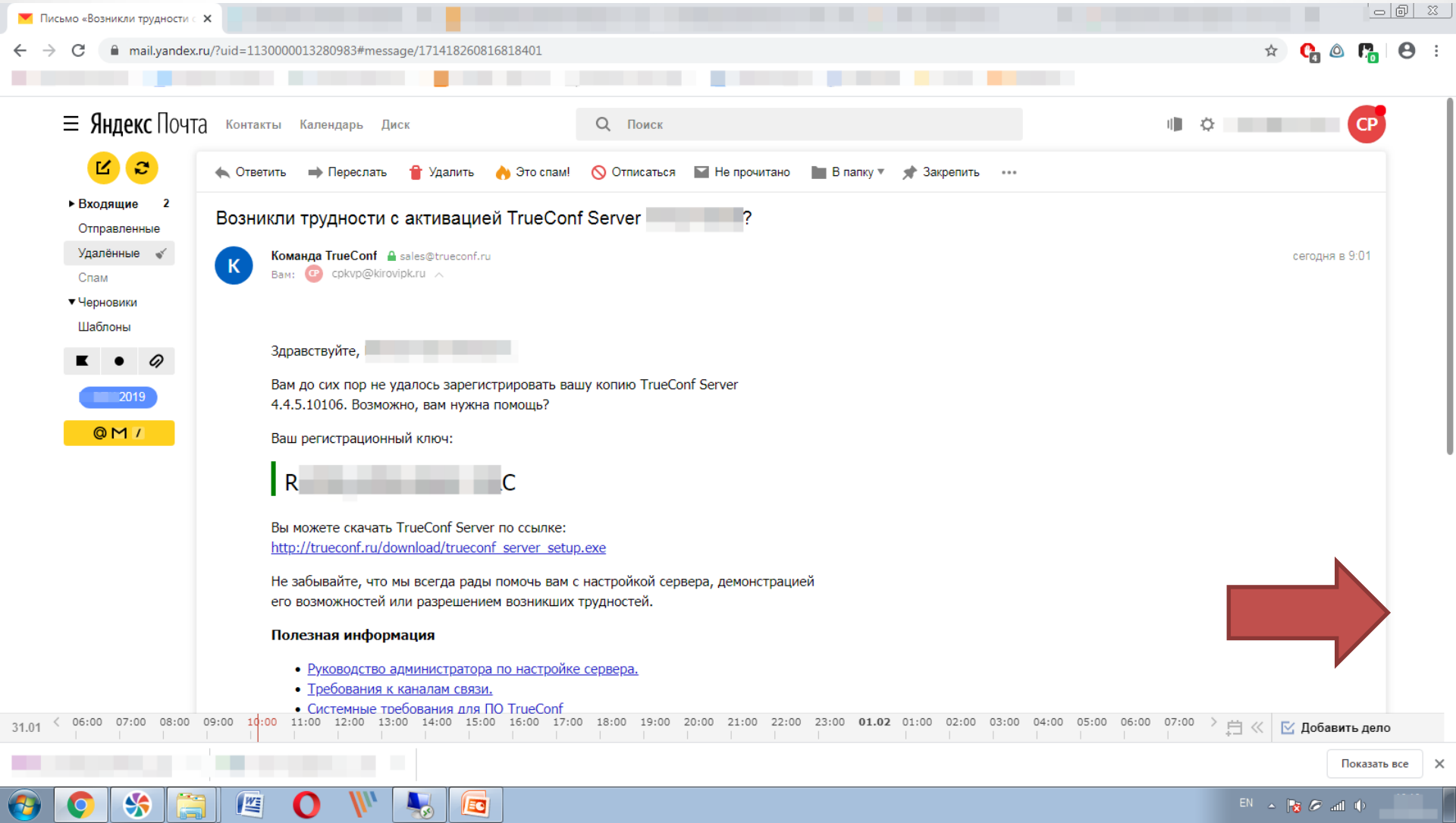
Не доверяйте непроверенным Wi-Fi-соединениям, которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей.

- работа в личных кабинетах
- открытие приложений онлайн банков
- социальные сети

Рассылка о смене пароля

Банки, интернет магазины, различные сервисы никогда не рассылают писем с просьбой **перейти по ссылке**, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные.

Рекламные и навязчивые рассылки



ПРИМЕР

- Руководство администратора по настройке сервера.
- Требования к каналам связи.
- Системные требования для ПО TrueConf

Желаем вам отличных видеоконференций,
Команда TrueConf

+7 (495) 698-60-66
sales@trueconf.ru
https://trueconf.ru

Вы получили это письмо, потому что вы подавали заявку на получение регистрационного ключа для TrueConf Server. Если вы больше не желаете получать письма от TrueConf - перейдите по ссылке.

ПРИМЕР

Вы получили это письмо на адрес vasev-vp@ya.ru, потому что подписались на рассылку на нашем сайте www.litres.ru или через мобильные приложения ЛитРес. Настроить параметры рассылки можно в личном кабинете. Чтобы отписаться от рассылки прямо сейчас, нажмите сюда.

If you do not wish to receive further communications like this, please click here to unsubscribe.

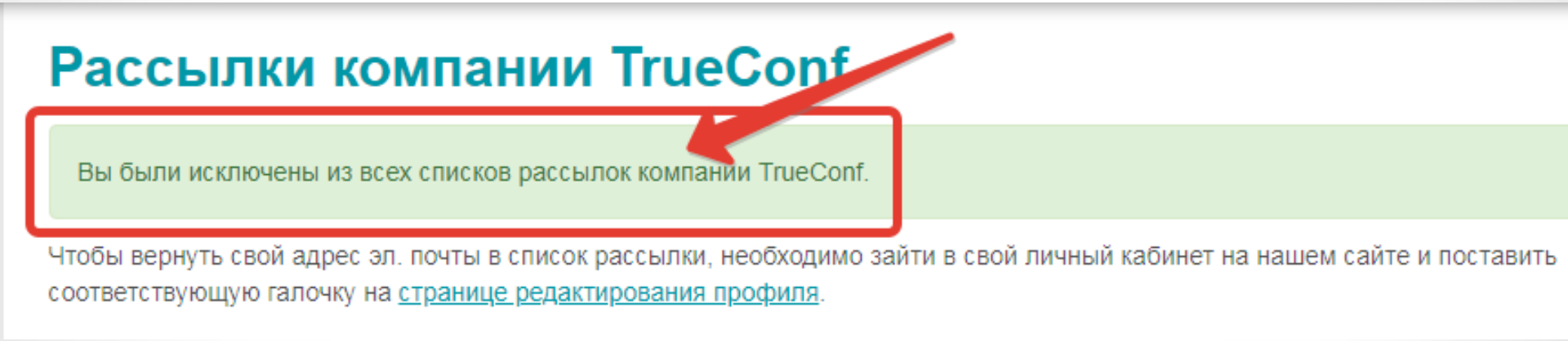
ООО "ЛитРес", ИНН 7719571260, ОГРН 1057748936398, 8 (800) 333-27-37

Юридический адрес: 123022, Москва, ул.2-я Звенигородская д.13 стр.41

Политика конфиденциальности

Хочу получать рассылку реже

ПРИМЕР


Рассылки компании TrueConf
Вы были исключены из всех списков рассылок компании TrueConf.
Чтобы вернуть свой адрес эл. почты в список рассылки, необходимо зайти в свой личный кабинет на нашем сайте и поставить соответствующую галочку на странице редактирования профиля.

Использование нескольких адресов электронной почты

Используйте отдельную электронную почту для официальной переписки.

Для остальных целей следует завести новую электронную почту.

Для каждой электронной почты необходимо создать сложный пароль.

Если в секретном вопросе вы указали **девичью фамилию матери**, которая сейчас есть в открытом доступе на ее страницах в соцсетях, обязательно поменяйте секретный вопрос.

Антивирусное ПО

Установите и обновляйте антивирусное ПО. Устаревшие версии не могут гарантировать защиту от вредоносного ПО. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.

Важный момент: в антивирусном ПО нуждаются не только настольные ПК, но и планшеты, смартфоны.

Открытие сторонних ссылок

Кликать по ссылкам, пришедшим в сообщениях от незнакомых людей — верный способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного знакомого, поэтому лучше уточните, что такое он вам прислал и нужно ли это открывать.

Внимательно проверяйте адреса ссылок, логотипы, текст и отправителя сообщений.

! Никогда не отвечайте на спам.

! Не запускайте неизвестные файлы, особенно с расширением .exe

Просьба от сына / дочки / внука

При получении сообщения с просьбой от знакомого срочно выслать денег, ничего не отправляйте. Для начала перезвоните и удостоверьтесь, что аккаунт не был взломан злоумышленниками.

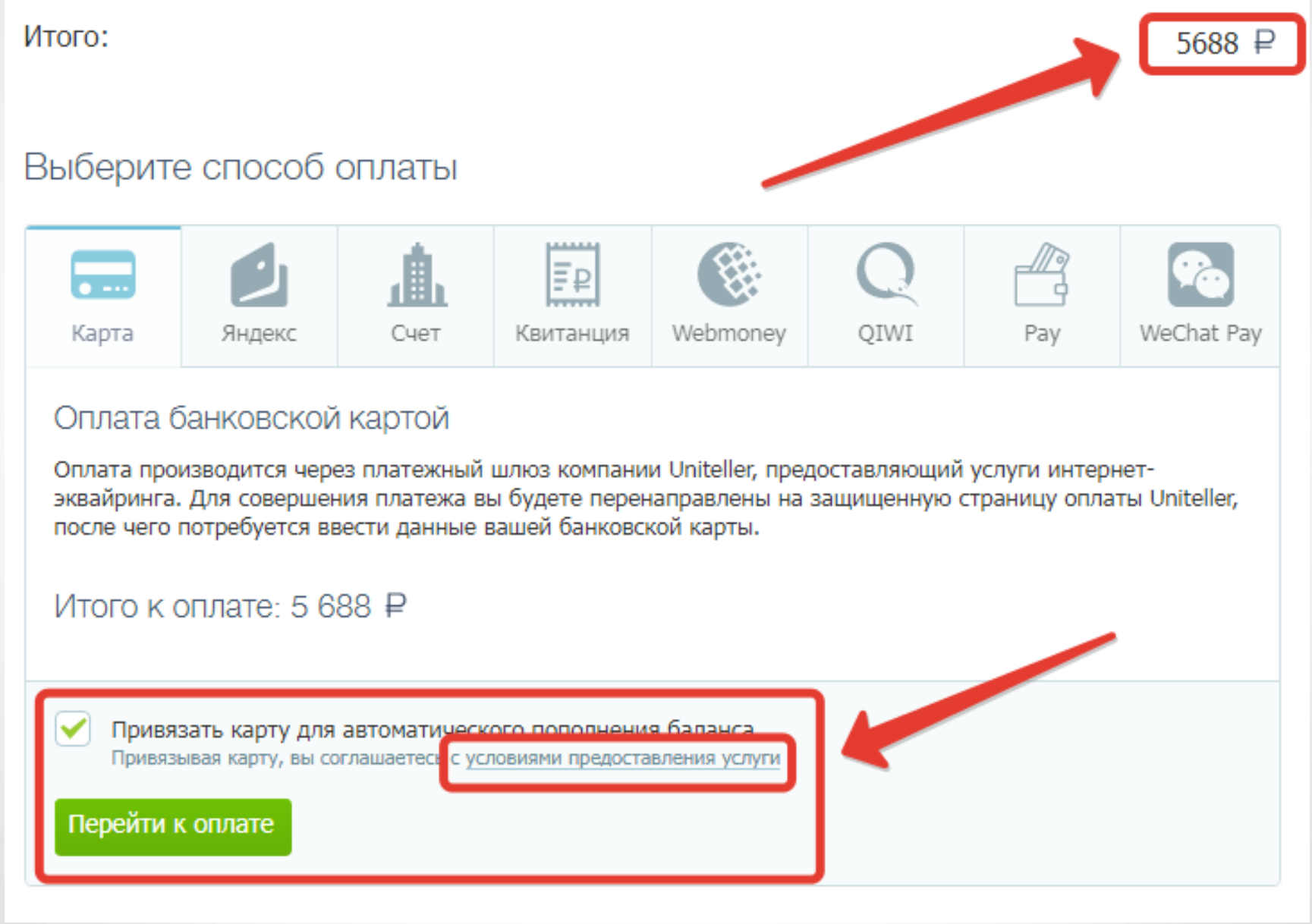
Сохраняйте резервные копии данных

Регулярно выполняйте резервное копирование данных. Следуйте правилу «3-2-1»: создайте одну основную копию и две резервные. Сохраните две копии на разных физических носителях, а одну — в облачном хранилище (Google Диск, Яндекс.Диск). Не забывайте «бэкапить» смартфоны, планшеты, компьютеры / ноутбуки.

Читайте «мелкий шрифт»

При оплате каких либо услуг, товаров и т.д., внимательно изучайте правила покупки, прежде чем сразу нажимать чекбокс **«СОГЛАСЕН С ПРАВИЛАМИ, ОПЛАТИТЬ».**

Часто при оплате, перед финальным нажатием кнопки «**оплатить»,** сумма может измниться в большую сторону.


Итого:
5688 ₽
Выберите способ оплаты
Карта
Яндекс
Счет
Квитанция
Webmoney
QIWI
Pay
WeChat Pay
Оплата банковской картой
Оплата производится через платежный шлюз компании Uniteller, предоставляющий услуги интернет-эквайринга. Для совершения платежа вы будете перенаправлены на защищенную страницу оплаты Uniteller, после чего потребуется ввести данные вашей банковской карты.
Итого к оплате: 5 688 ₽
Привязать карту для автоматического пополнения баланса
Привязывая карту, вы соглашаетесь с условиями предоставления услуги
Перейти к оплате

Те самые «условия» предоставления услуги:

При подключении возможности пополнения баланса с карты списание денежных средств с привязанной карты будет производиться в автоматическом режиме.

Списание с карты будет происходить за 10 дней до окончания средств на балансе. Сумма списания равна платежу за 1 месяц предоставления услуги.

Уведомление о каждом списании (успешном или неуспешном) по e-mail и СМС не предусмотрено. Предварительное уведомление по e-mail и СМС об окончании средств на балансе больше не производится.

В случае, если автоматическое списание не удалось, то повторное списание будет произведено через 24 часа. Попытки будут повторяться, пока баланс не пополнится или аккаунт не будет заблокирован.

Если с момента последнего автоматического списания прошло 179 дней, то будет произведен перепривязочный платеж на 90 копеек. Средства будут возвращены на карту в течение 4-7 рабочих дней.

Не забываем про детей

Установите безопасный режим для ребенка. Для этого создайте отдельную учетную запись на сайте выбранной вами поисковой системы или используйте детские поисковики: Гогуль. (**Первый специализированный детский интернет-браузер)** (http://gogul.tv)). При помощи нового браузера, разработанного компанией «Новое поколение», дети могут посещать только одобренные родителями и учителями сайты, которые занесены в базу данных. Сейчас в этой базе уже около семи тысяч сайтов с более чем 500 тысячами фотографий и видеороликов. В «Гогуле» не применяются сложные алгоритмы для контроля родителей над ресурсами, он работает по принципу «всё, что не разрешено, запрещено».

Не скачивайте сомнительные приложения

Не скачивайте сомнительные приложения и не пытайтесь это делать по неизвестным ссылкам. Пользуйтесь только официальными магазинами App Store, Google Play и Windows Market.

Все же на данных ресурсах есть приложения которые могут принести вред, поэтому внимательно изучаем информацию о продукте, о создателе, его рейтинг, отзывы.

Не совершайте покупки в социальных сетях

Крайне не рекомендуется совершать покупки в социальных сетях. Данные покупки подразумевают перевод денежных средств на счет физических лиц, чаще с предоплатой. Для таких приобретений существуют проверенные интернет магазины.

При частых покупках через Интернет, лучше завести отдельную банковскую карту (обязательно СМС оповещение), или отдельный счет, например Яндекс деньги.

Сервис Яндекс деньги, доступен любому пользователю, имеющему электронную почту на «Yandex».

Записи и сообщения в социальных сетях на тему спасения животных

Не делайте в социальных сетях репостов объявлений про бедного милого котика, который срочно ищет дом (а в посте — телефон владельца или номер карты, куда можно перечислить деньги на содержание животного). Велика вероятность, что это мошенники, решившие заработать на сердобольных и доверчивых гражданах.

При желании оказать помощь, проверяйте информацию о службе в своем городе (когда создан, кто руководитель и т. д.).

Обращайте внимание на адрес сайта

Здесь речь идет о существовании большого количества поддельных сайтов.

Обращайте внимание на адрес страницы, которую вы часто посещаете / посетили впервые:

если адрес отличается хотя бы на один символ

(например:

https://www.tcinet.ru/ - оригинал

https://www.tsinet.ru/ - подделка

введите его вручную.

Проверить, когда был создан сайт, можно здесь.

Sim карта и телефон

При появлении на смартфоне надписи **«Вставьте сим-карту»**, зайдите в ближайший офис мобильного оператора или позвоните ему с другого телефона и выясните, в чем проблема. Возможно, кто-то получил дубликат вашей sim карты и ее нужно срочно заблокировать.

! При потере телефона, блокируйте и телефон с sim картой и саму банковскую карту.

! Наличие пароля (разблокировка по лицу, графический ключ, отпечаток пальца) для разблокировки смартфона строго обязательно.

Отправка СМС на номер

Мошенниками могут быть созданы сайты, на которых вы якобы можете бесплатно и неограниченно смотреть или скачивать приглянувшиеся фильмы, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров. Помним об авторских правах.

Продление подписки

Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего вы должны самостоятельно отключить услугу. Если вы этого не сделаете, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.