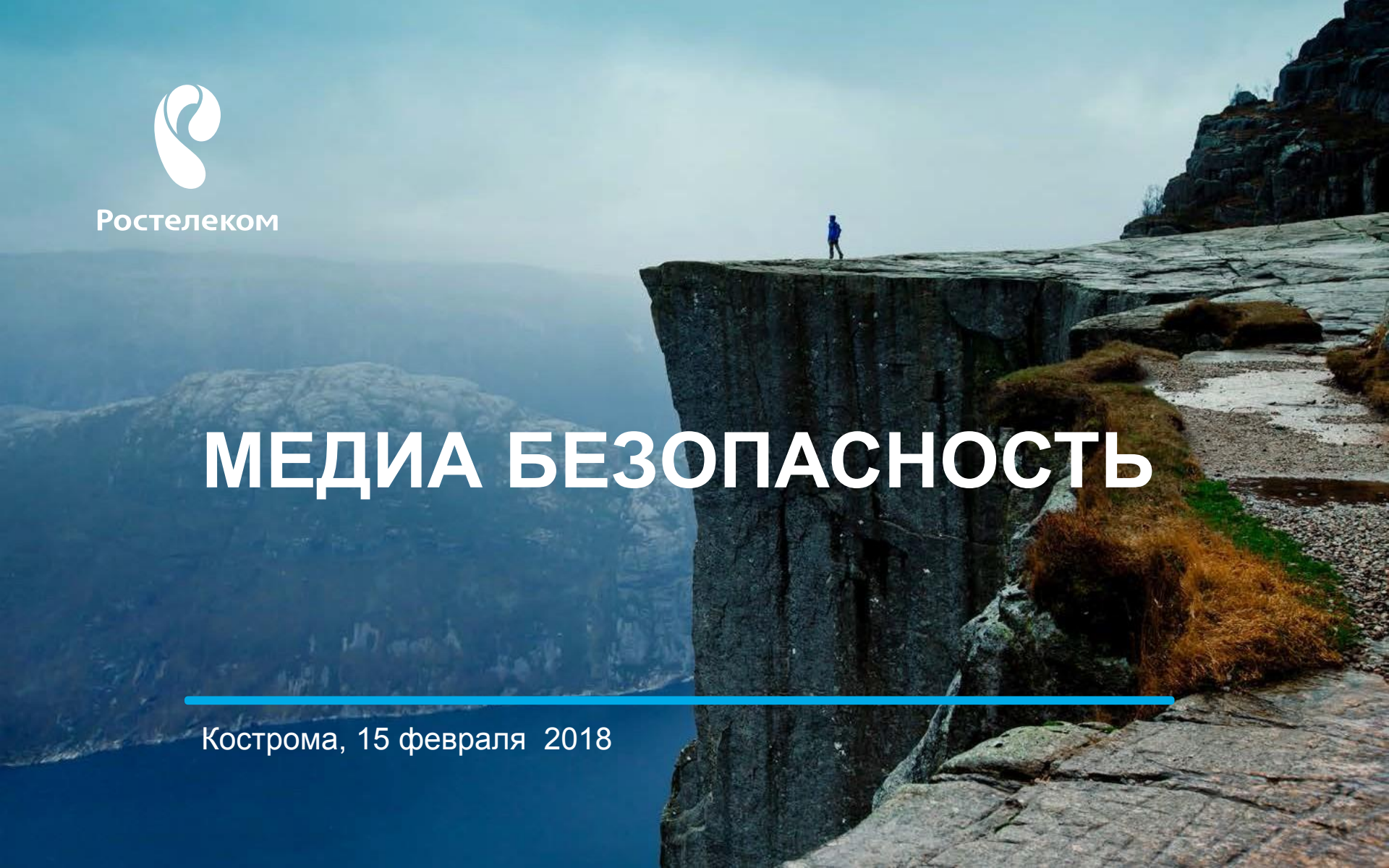
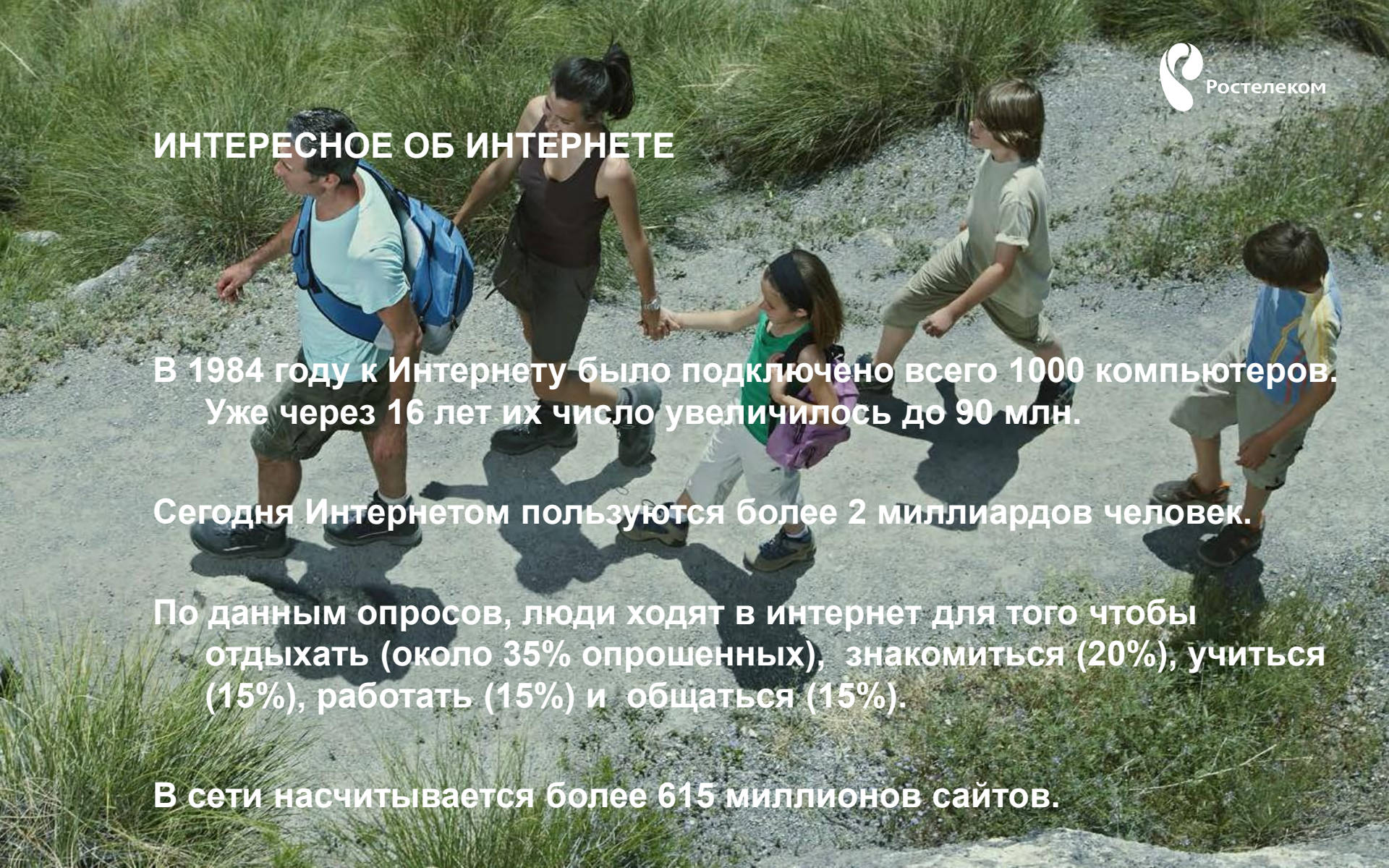


МЕДИА БЕЗОПАСНОСТЬ

Кострома, 15 февраля 2018



Ростелеком

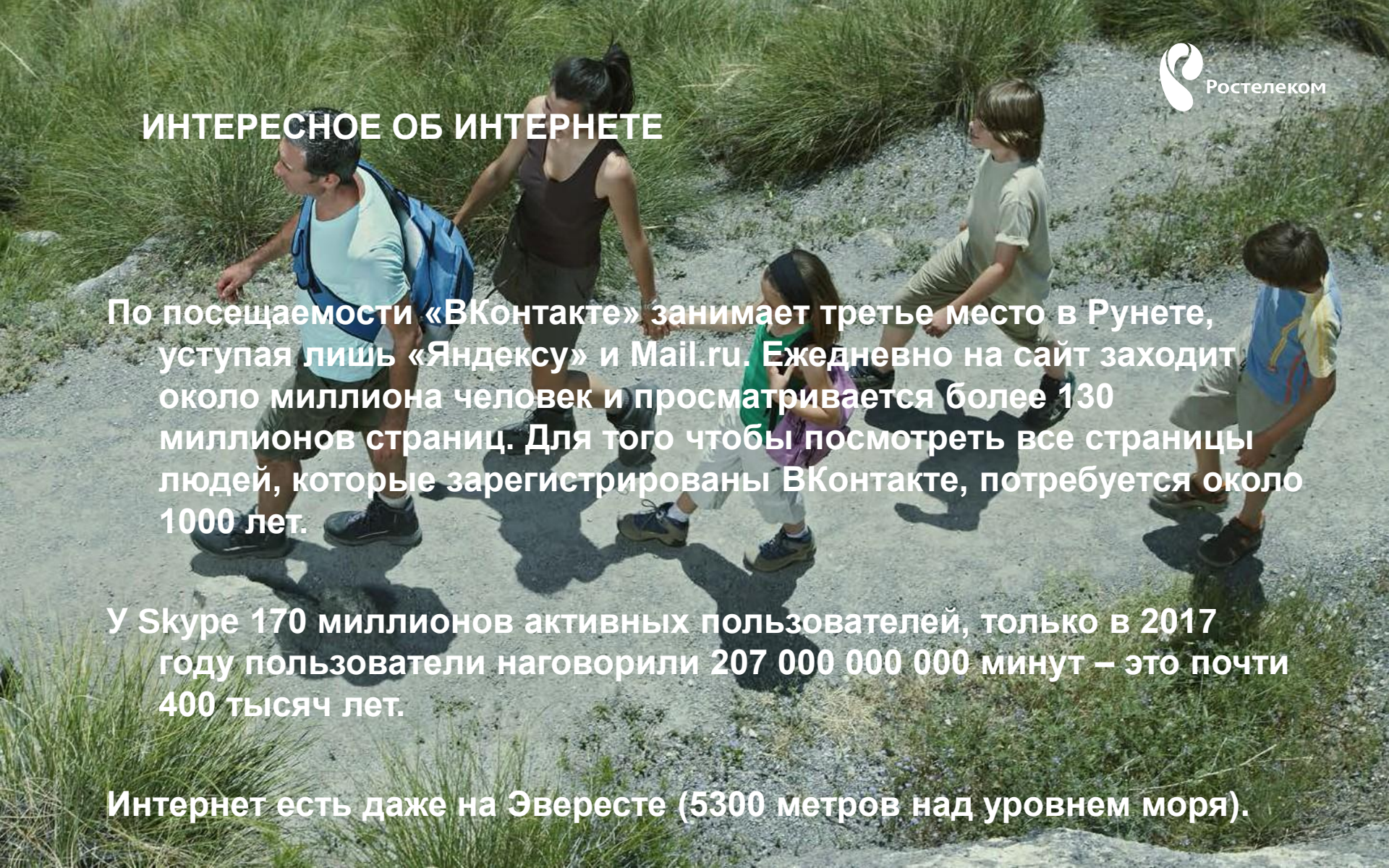
ИНТЕРЕСНОЕ ОБ ИНТЕРНЕТЕ

В 1984 году к Интернету было подключено всего 1000 компьютеров. Уже через 16 лет их число увеличилось до 90 млн.

Сегодня Интернетом пользуются более 2 миллиардов человек.

По данным опросов, люди ходят в интернет для того чтобы отдыхать (около 35% опрошенных), знакомиться (20%), учиться (15%), работать (15%) и общаться (15%).

В сети насчитывается более 615 миллионов сайтов.



ИНТЕРЕСНОЕ ОБ ИНТЕРНЕТЕ

По посещаемости «ВКонтакте» занимает третье место в Рунете, уступая лишь «Яндексу» и Mail.ru. Ежедневно на сайт заходит около миллиона человек и просматривается более 130 миллионов страниц. Для того чтобы посмотреть все страницы людей, которые зарегистрированы ВКонтакте, потребуется около 1000 лет.

У Skype 170 миллионов активных пользователей, только в 2017 году пользователи наговорили 207 000 000 000 минут – это почти 400 тысяч лет.

Интернет есть даже на Эвересте (5300 метров над уровнем моря).

Когда появился Интернет и как расшифровывается “www”?

World Wide Web, WWW — Всемирная паутина

В 1957 году Министерство обороны США посчитало, что на случай войны нужна надежная система передачи информации. Компьютерная сеть была названа ARPANET и в 1969 году сеть объединила научные учреждения, которые занимались разработкой этого проекта.

К 1971 году была разработана первая программа для отправки электронной почты по сети. В 1973 году сеть стала международной.

В 1984 году была разработана система доменных имен.

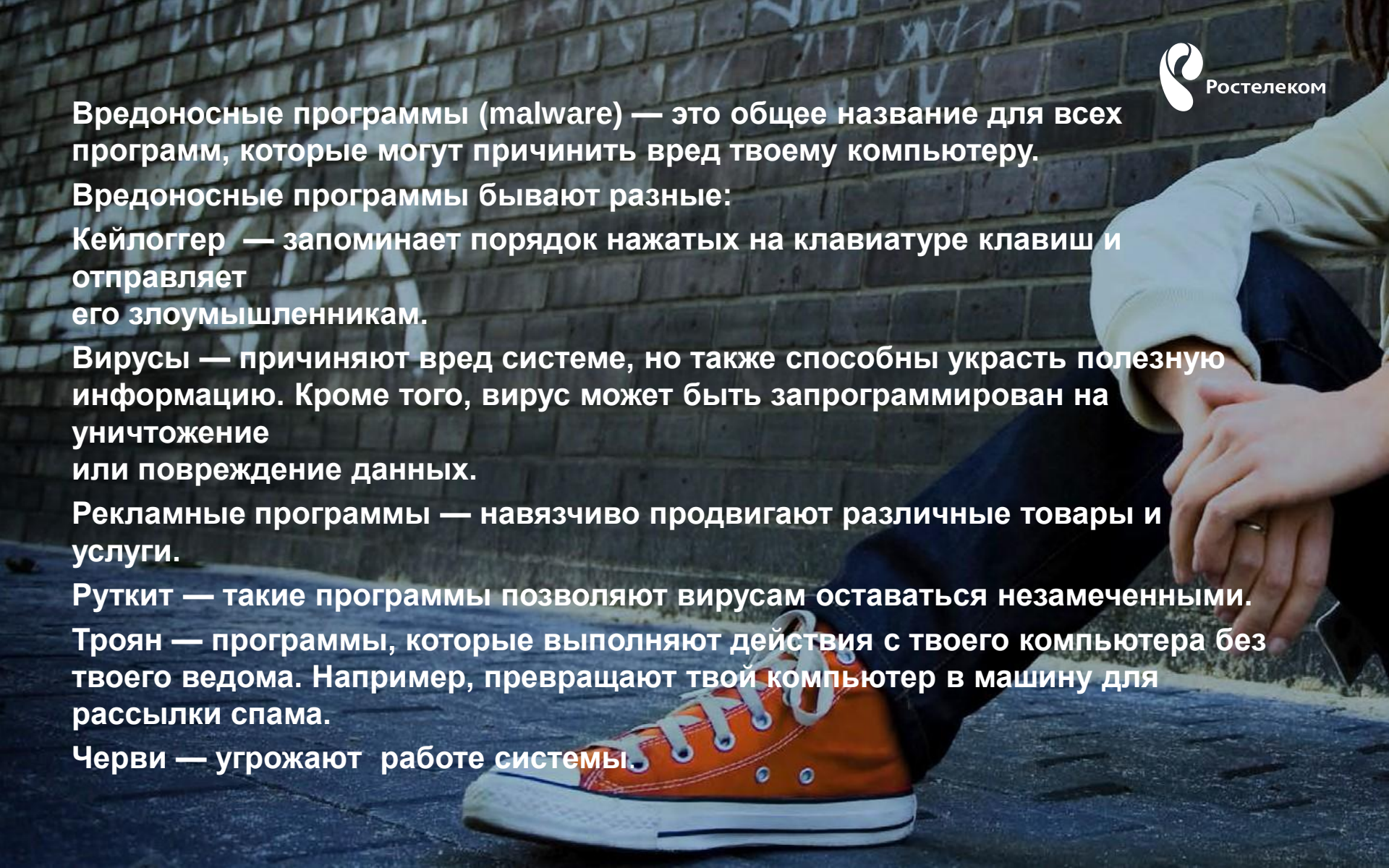
В 1988 году в Интернете стало возможно общение в режиме реальном времени (чат).

В 1989 году в Европе родилась концепция Всемирной паутины.

В 1990 году сеть ARPANET прекратила свое существование. В том же году было зафиксировано первое подключение к Интернету по телефонной линии.

В 1991 году Всемирная паутина стала общедоступна.


Ростелеком
Какие бывают вредоносные программы? Опиши их.



Вредоносные программы (malware) — это общее название для всех программ, которые могут причинить вред твоему компьютеру.

Вредоносные программы бывают разные:

Кейлоггер — запоминает порядок нажатых на клавиатуре клавиш и отправляет
его злоумышленникам.

Вирусы — причиняют вред системе, но также способны украсть полезную информацию. Кроме того, вирус может быть запрограммирован на уничтожение
или повреждение данных.

Рекламные программы — навязчиво продвигают различные товары и услуги.

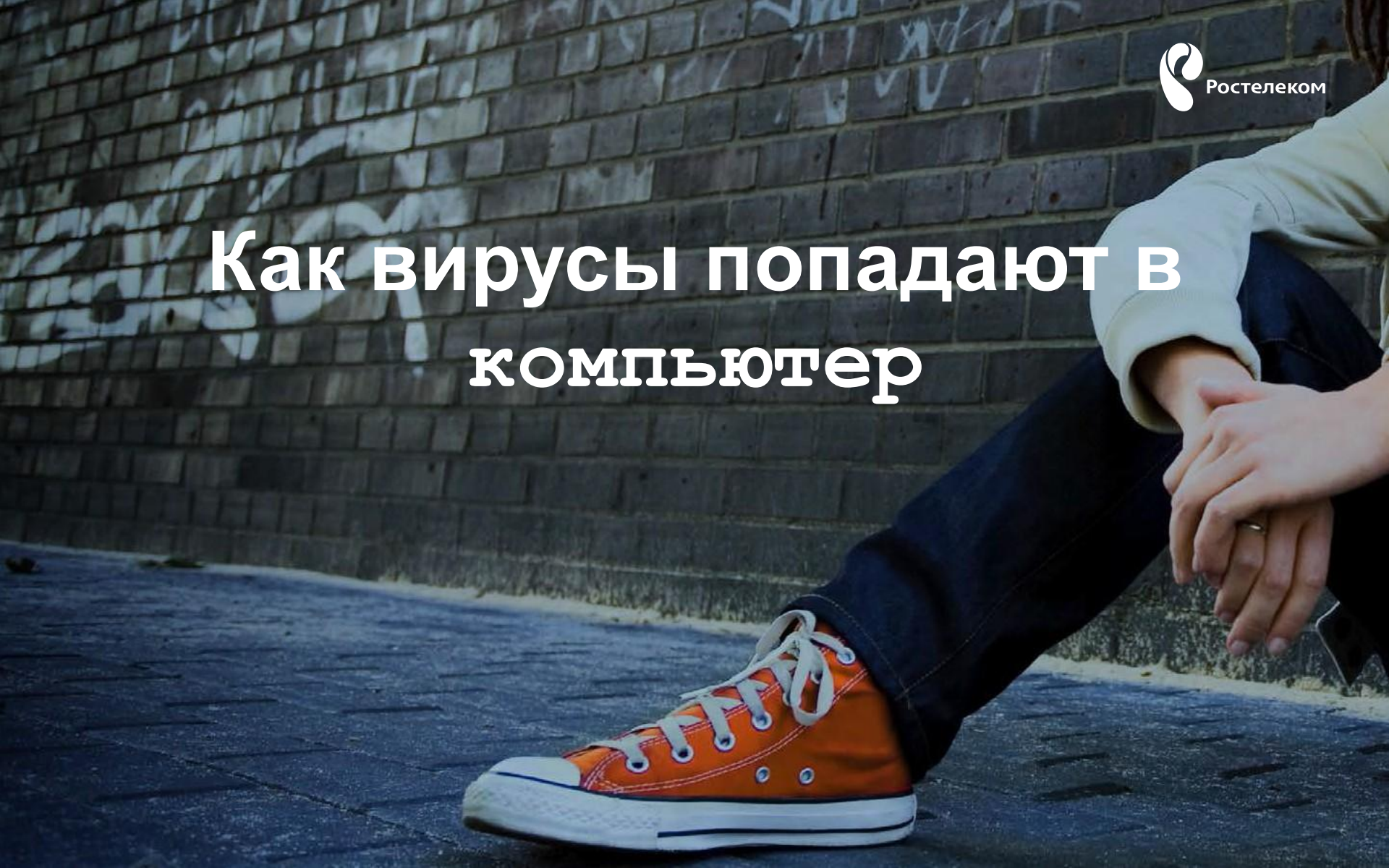
Руткит — такие программы позволяют вирусам оставаться незамеченными.

Троян — программы, которые выполняют действия с твоего компьютера без твоего ведома. Например, превращают твой компьютер в машину для рассылки спама.

Черви — угрожают работе системы.

Бэкдор (средство удаленного администрирования).
Бэкдор, или RAT (remote administration tool), — это приложение, которое позволяет честному системному администратору или злобному злоумышленнику управлять вашим компьютером на расстоянии. В зависимости от функциональных особенностей конкрентного бэкдора, хакер может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру. Словом, брать на себя контроль за компьютером и информацией жертвы.

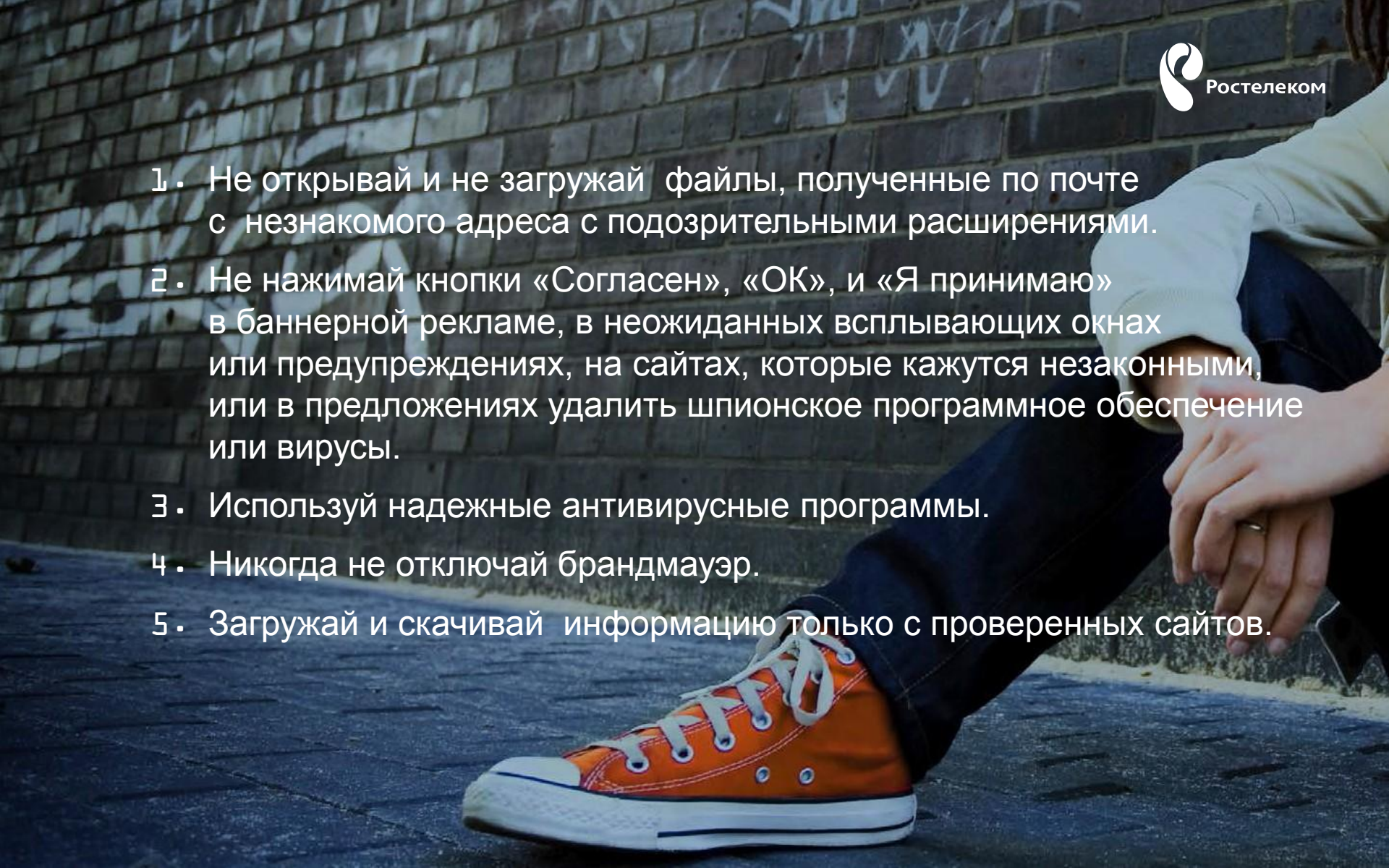
Загрузчик - эта зараза является небольшой частью кода, используемой для дальнейшей загрузки и установки полной версии вредоноса. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь вредонос.


Ростелеком
Как вирусы попадают в компьютер

Основные лазейки, по которым вирусы «пробираются» в компьютер

• уязвимости браузеров;
• сбои в операционной системе;
• флешки и переносные внешние жесткие диски;
• электронная почта;
• программы мессенджеры (Skype, Mail.ru-Агент, ICQ и т.д.).


Ростелеком
Как защитить свой компьютер от вредоносных программ?



1. Не открывай и не загружай файлы, полученные по почте с незнакомого адреса с подозрительными расширениями.
2. Не нажимай кнопки «Согласен», «ОК», и «Я принимаю» в баннерной рекламе, в неожиданных всплывающих окнах или предупреждениях, на сайтах, которые кажутся незаконными, или в предложениях удалить шпионское программное обеспечение или вирусы.
3. Используй надежные антивирусные программы.
4. Никогда не отключай брандмауэр.
5. Загружай и скачивай информацию только с проверенных сайтов.

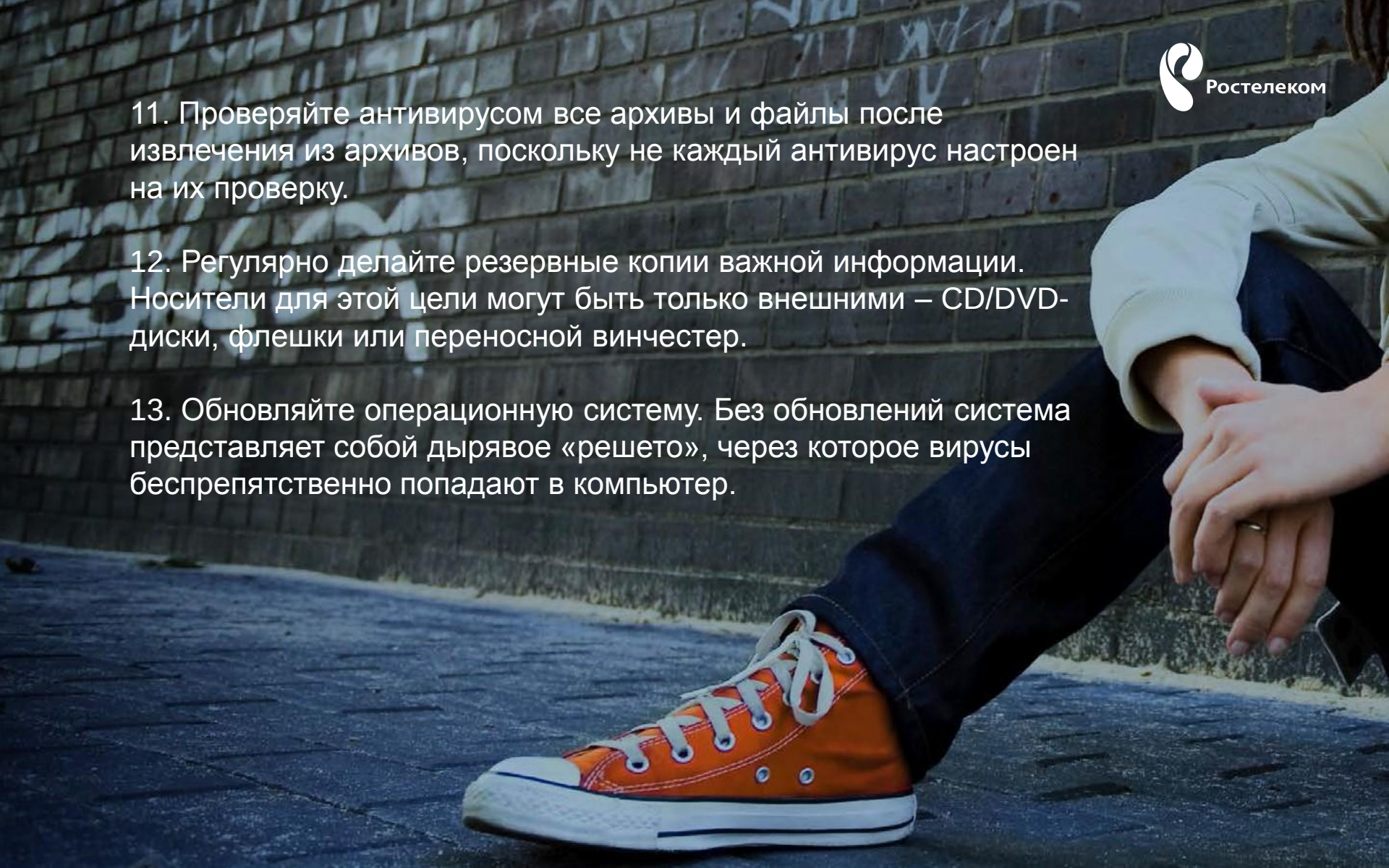
6. Не посещай подозрительные сайты
Подавляющее большинство из них содержат вирусы, непременно атакующие твой компьютер при первом же посещении.

7. Используй современные операционные системы, не дающие
изменять важные файлы без ведома пользователя.

8. Используй внешние носители информации только от проверенных
источников.

9. Своевременно устанавливай обновления.

10. Используй надежные пароли (с большим количеством символов)
и храни их в секрете.



11. Проверяйте антивирусом все архивы и файлы после извлечения из архивов, поскольку не каждый антивирус настроен на их проверку.

12. Регулярно делайте резервные копии важной информации. Носители для этой цели могут быть только внешними – CD/DVD-диски, флешки или переносной винчестер.

13. Обновляйте операционную систему. Без обновлений система представляет собой дырявое «решето», через которое вирусы беспрепятственно попадают в компьютер.

Что такое нелегальный контент и почему его иногда называют пиратским?

У любого созданного произведения есть свой автор.

Программы, музыка, книги, игры, рефераты, тексты, мультимедийные файлы, презентации и т.д. — все это является объектом авторского права
и охраняется законом. И этот закон ты нарушаешь, если скачиваешь явно незаконные копии того или иного произведения (например, фильм, который еще только идет в кинотеатре, в интернете явно выложен с нарушением закона!) или выкладываешь их сам на различные сетевые ресурсы.

Пираты — это те, кто незаконно присваивают себе чужое!

Использование термина «пиратство» по отношению к нарушению авторских прав имеет давнюю историю. Первые его упоминания относятся аж к XVII веку!

Ростелеком

Чем опасно скачивание пиратского контента?

Ростелеком

Многие интернет-ресурсы (например, социальные сети) построены таким образом, что их владельцы предоставляют пользователям возможность самим размещать (англ. — содержимое) — любое информационно значимое наполнение информационного ресурса).

При этом в большинстве случаев обязательным условием для регистрации на том или ином сайте является согласие пользователя с правилами, установленными его владельцем.

Одним из обязательных положений таких правил является то, что пользователь может размещать только тот контент, законным правообладателем которого он является.

Ростелеком

Поэтому, если ты размещаешь где-то, например, новую песню любимого исполнителя, имей в виду, что ответственность за нарушение авторского права несешь ты, а не владелец ресурса!

Ответственность за нарушение авторских прав зависит от характера осуществляемых действий и бывает:

гражданско-правовая (Гражданский кодекс, часть IV),

административная (Кодекс об административных правонарушениях, Статья 7.12),

и даже **уголовная** (Уголовный кодекс, статья 146)!

Ростелеком

Какие виды мошенничества в Интернете существуют?

Мошенничество — это обман, способ добычи денежных средств и других ценностей, основанный на доверчивости граждан. В простонародье мошенничество еще называют –**лохотрон**.

«Попрошайки в сети»
Обычно люди просят незначительную сумму денег, объясняя причину их надобности или необходимости им.
Предлоги могут быть совершенно разные, от срочной операции, необходимой ребенку, до покупки корма собаке.
Суммы зачастую мизерные, ведь так больше шансов получить «пожертвование», собрать денег с большего количества народа. Обычно используются рассылки писем (спама) на e-mail жертв.

Чудо-методики заработка

Тебе предлагают купить некую секретную методику, которая позволяет зарабатывать 100–150$ в день, практически ничего не делая.

Письма счастья

Из письма ты вдруг узнаешь, что выиграл в лотерею или что-то в таком духе, но для того, чтобы получить выигрыш нужно оплатить какой-то налог.

СМС-мошенничество

Тебе предлагают купить гороскоп или способ похудеть, прочитать чужие смски или сообщения в социальной сети, а за это тебе нужно отослать смс на короткий номер**.**

Кардинг

Мошенники стараются, как можно быстрее, получить доступ к твоей банковской карте, для этих целей используют фиктивные интернет-магазины.

Списки кошельков

Тебе могут предложить отправить небольшие суммы денег на некоторое количество кошельков, потом вписать в список свой кошелек и распространять его дальше по форумам, доскам объявлений и т.д.

Фишинг

Пользователя направляют на какой-либо поддельный сайт, который с виду похож на сайт какого-то известного сервиса, платежной системы и т.д., чтобы человек ввел там свой пароль

Фарминг — это более «продвинутая» версия фишинга. Смысл заключается опять же в направлении пользователя на другой сайт, но это делается уже не через поддельные ссылки.

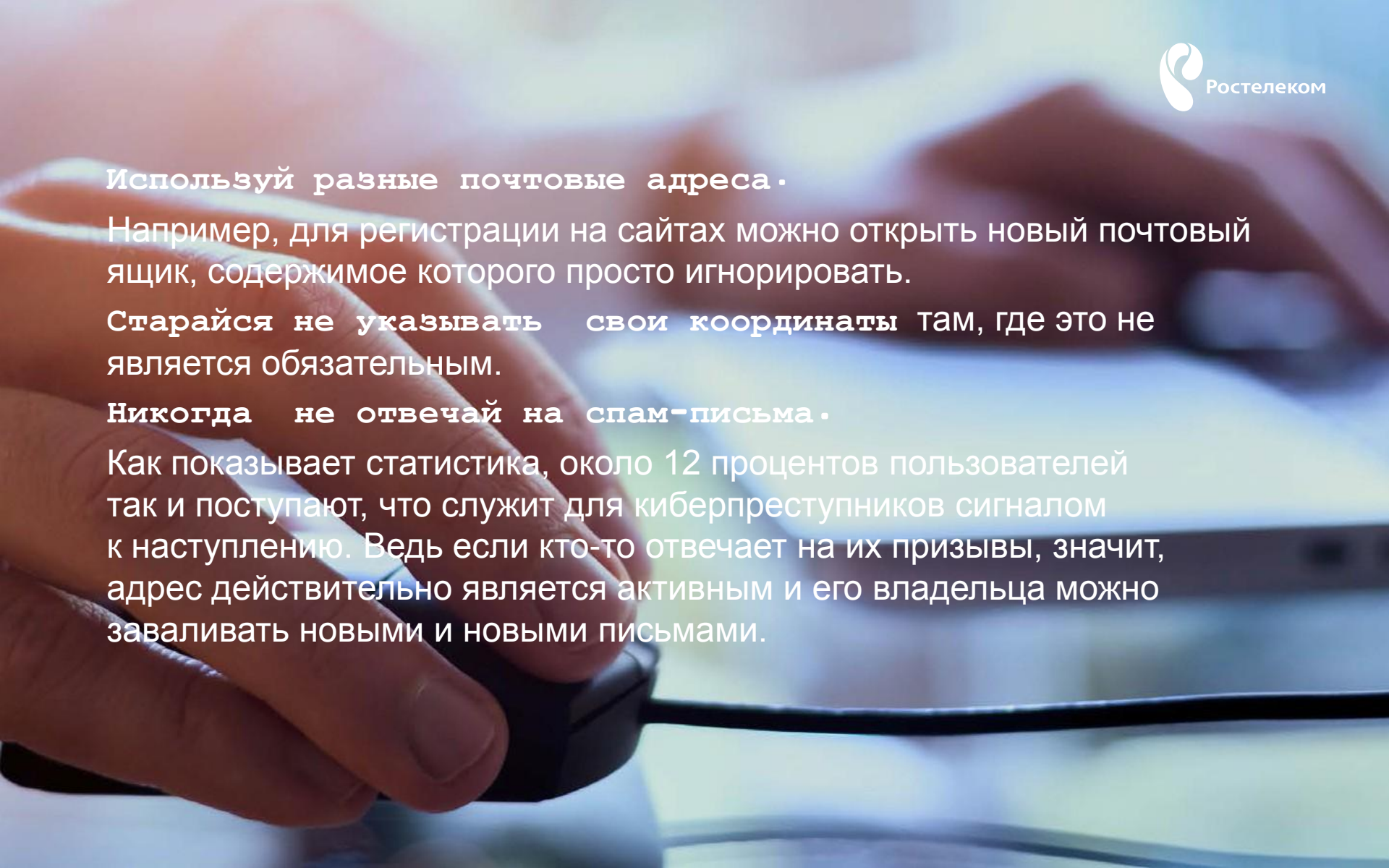
Взломы аккаунтов

Вконтакте, фейсбук и других социальных сетях сегодня практически у каждого пользователя интернета имеются свои аккаунты в этих сетях.
Мошенничество здесь заключается в том, что при попытке входа в социальную сеть для разблокировки своего аккаунта Вас просят отправить смс на какой-либо номер.
Ни в коем случае не делайте этого! За эту смску с Вас снимут немалые деньги.

Мошенничество, связанное с распространением софта

Смысл состоит в том, что при выходе какой-либо новой программы, игры, фильма и т.п. новинки появляются на торрент-треккерах.
Человек скачивает этот софт, затем запаковывает в архив, который защищает паролем и распространяет его в сети. Выкладывает под видом бесплатного!
Вы скачиваете такой архив, а при распаковке он требует указать пароль.
Для получения пароля отправьте смс на номер…


Ростелеком
Как защитить себя от спама в Интернете?



Используй разные почтовые адреса.

Например, для регистрации на сайтах можно открыть новый почтовый ящик, содержимое которого просто игнорировать.

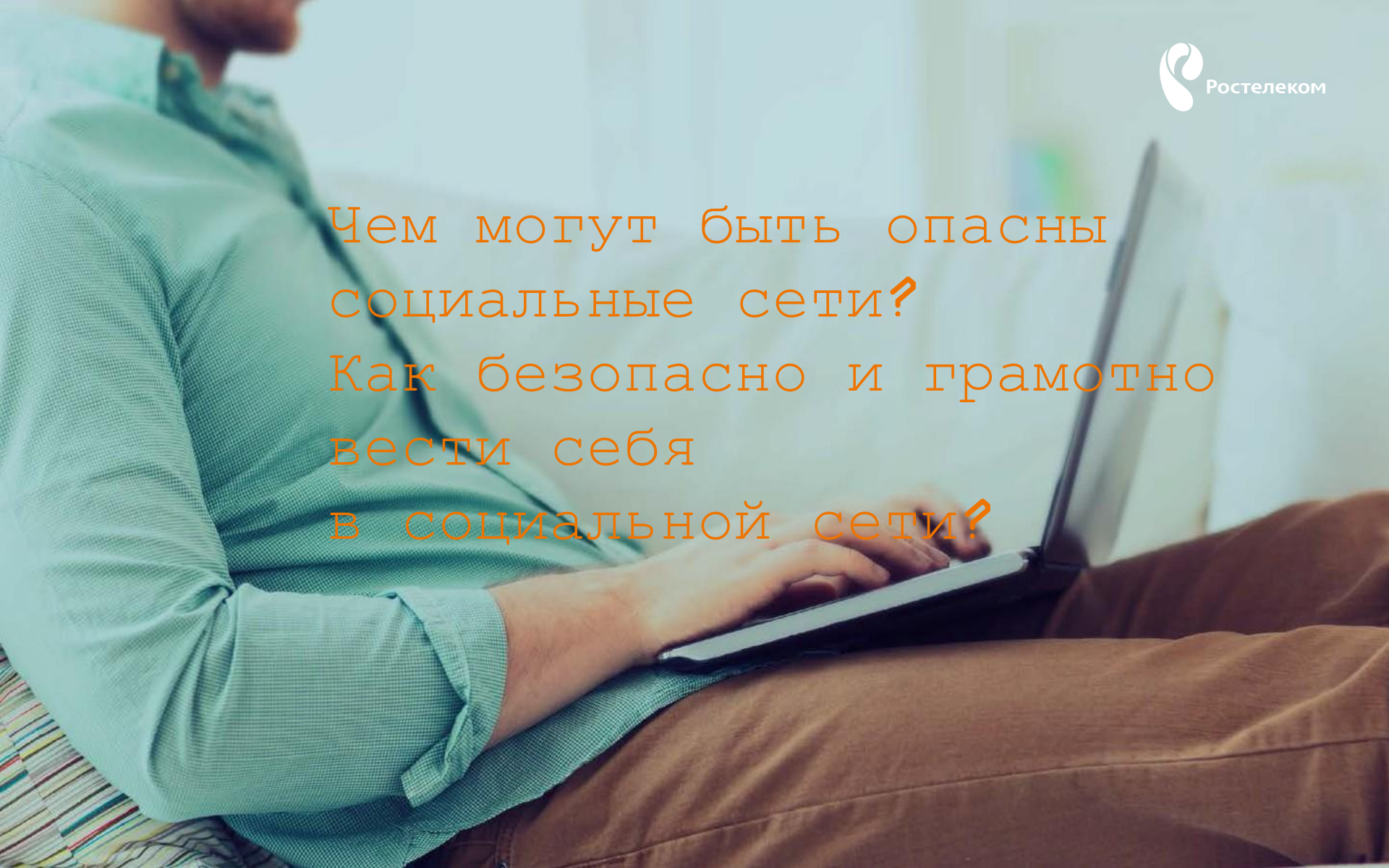
Старайся не указывать свои координаты там, где это не является обязательным.

Никогда не отвечай на спам-письма.

Как показывает статистика, около 12 процентов пользователей так и поступают, что служит для киберпреступников сигналом к наступлению. Ведь если кто-то отвечает на их призывы, значит, адрес действительно является активным и его владельца можно заваливать новыми и новыми письмами.

Как правильно совершать покупки в Интернете?

1. **Покупай только в надежных, проверенных местах.**
2. **Внимательно и полностью прочитай описание продукта.**
3. **Обрати внимание на цену, учти стоимость доставки!**
4. **Не доверяй чересчур низким ценам!**
5. **Не бойся звонить и уточнять!**
6. **Выбери проверенную службу доставки.**


Ростелеком
Чем могут быть опасны социальные сети?
Как безопасно и грамотно вести себя в социальной сети?

Топ-5 любопытных фактов о подростках и Интернете

1.Ученые доказали, что подростки, которые проводят в Интернете от 4 часов в день, страдают депрессией и имеют низкую самооценку.

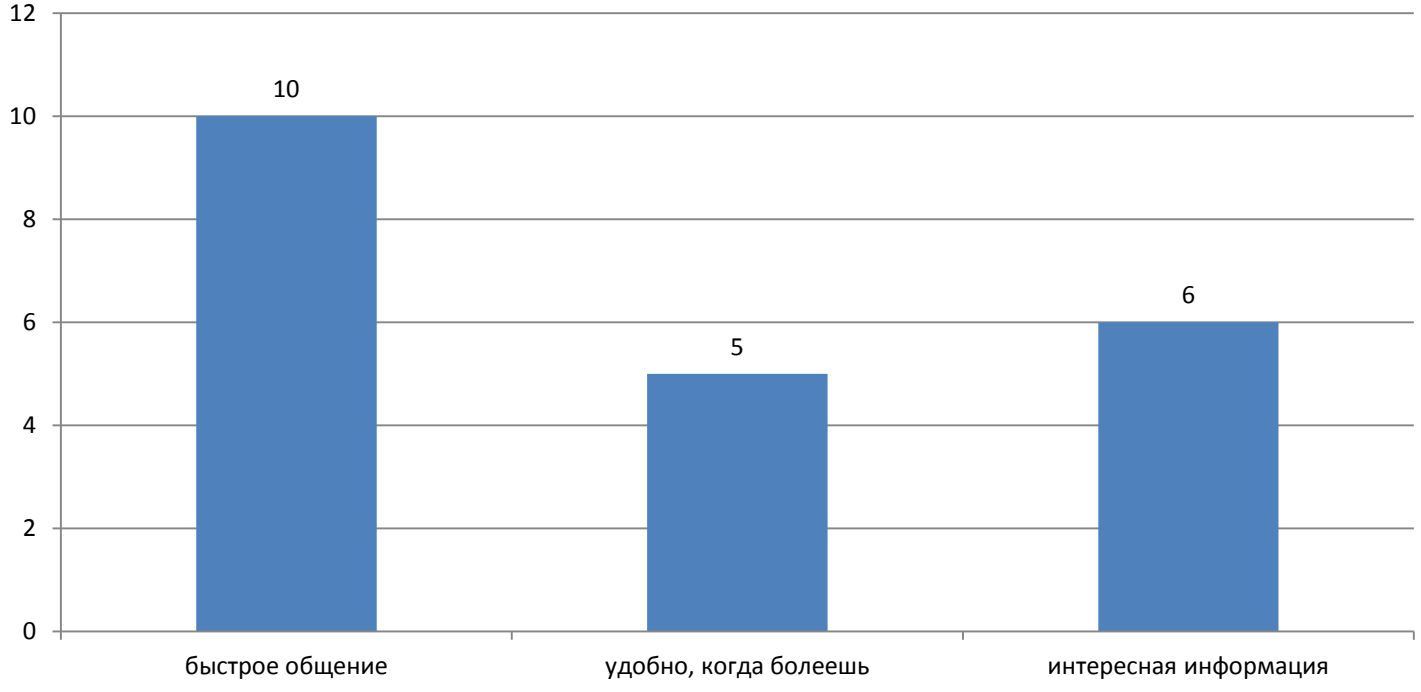
2.Психиатры выяснили, что постоянное желание обновить страничку в соц. сетях (компульсивное расстройство) доводит до депрессии.

3.Daily Mail выяснил, что учащиеся, которые во время подготовки к экзаменам или во время сессии, отвлекались на социальные сети, получили оценки на 20% ниже, чем те, кто не был увлечен соц. сетями и Интернетом.

4.По даным TNS Digital Life, Россия занимает второе место в мире по среднему времени, проводимому в соц. сетях, на душу населения.

5.Ещё одно исследование провели в медицинской школе Кливлендского университета. В ходе исследования выяснилось, что ученики, которые в школе отправляли более 120 сообщений в день, чаще страдают такими расстройствами как нарушение сна, депрессия, повышенная агрессивность.

В чем преимущества социальных сетей?



В чем недостаток социальных сетей?

Отнимает много времени – 100%

Опасность виртуального мира

Многие люди не понимают, что информация, размещённая ими в социальных сетях, может быть найдена и использована кем угодно, не обязательно с благими намерениями.

Информацию об участниках социальных сетей могут найти их работодатель, родственники, сборщики долгов, преступники и так далее. Судебные приставы иногда используют социальные сети, чтобы найти неплательщиков или получить сведения об их имуществе.

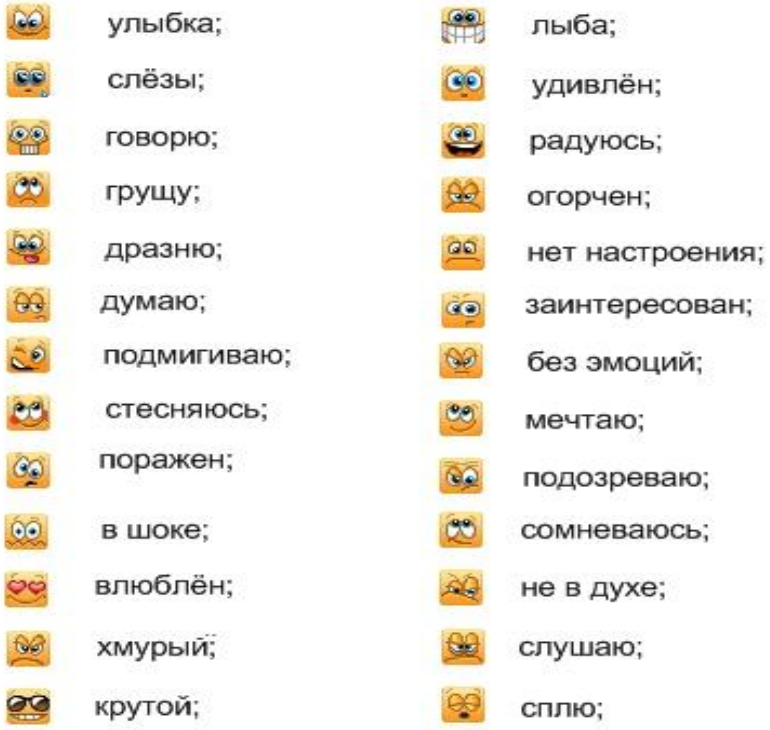
Некоторые работодатели запрещают пользоваться социальными сетями — не только ради экономии, но и чтобы воспрепятствовать утечке информации.

Что бывает???

Известен случай проявления психосоматических расстройств на почве зависимости от общения в социальных сетях — в Белграде пользователь Снежана Павлович (Snezhana Pavlović) попала в психиатрическую клинику после того, как её заметка в социальной сети Facebook не вызвала интереса среди её друзей. Врачи клиники назвали этот случай «синдром Снежаны», объясняя поведение пациентки как обычный стресс от неудовлетворенности социальной потребности индивидуума в современном мире.

- зависимость от виртуального мира, что приводит к аутизму и полной деградации личности, как составляющей общества.
- развивается фобия (страх) общения с реальными людьми.
- подмена истинных чувств и ощущений на виртуальные переживания.
- подростки становятся двуличными
- увеличение потенциальны жертвами обмана.
- снижение и упрощение уровня грамотности, сокращение и замена слов
- Современные технологии позволяют выйти в социальные сети с телефона. Поэтому многие ученики могут заходить туда даже на уроках. А это мешает образовательному процессу.
- безразличие к учебе, ухудшение оценок, нехватка времени для чтения художественной литературы и иного обогащения внутреннего мира.

Зачем писать слова?



Развивается безграмотность

Ростелеком

Социальные сети являются мощным инструментом маркетинговых исследований, поскольку пользователи добровольно публикуют информацию о себе, своих взглядах, интересах, предпочтениях и так далее. Ввиду этого рекламодатели могут весьма четко определять, каких именно пользователей заинтересует их объявление, и направить свои рекламные объявления конкретным пользователям, в зависимости от информации в их профилях (возраст, пол, место жительства и прочее). Такой тип рекламы получил название таргетированной (англ. «Target» — цель).

Объём рынка рекламы в социальных сетях неуклонно растет.

Виды рекламы: *медийная, контекстная и видеореклама*, маркетинговые проекты, в которых маркетологи создают профили для своих товаров и брендов в социальных сетях, создание виджетов.

1. НЕ РАЗМЕЩАЙ ИНФОРМАЦИЮ О ТВОЕМ АДРЕСЕ, ПАСПОРТНЫХ ДАННЫХ, РАСПОРЯДКЕ ДНЯ, СВОИХ ПЛАНАХ ИЛИ ПЛАНАХ РОДИТЕЛЕЙ.
   ЭТО МОЖЕТ СПРОВОЦИРОВАТЬ МОШЕННИКОВ.
2. НОМЕРА МОБИЛЬНЫХ И АСЕК — ТОЖЕ ИНФОРМАЦИЯ НЕ ДЛЯ ПОСТОРОННИХ ГЛАЗ. СПАМЕРЫ НЕ ДРЕМЛЮТ!
3. ТВОИ ФОТО ИЛИ ВИДЕО МОГУТ СМОТРЕТЬ И ПОСТОРОННИЕ ЛЮДИ. НЕ ВСЕ ОНИ ТЕ, ЗА КОГО СЕБЯ ВЫДАЮТ.
4. ОСТОРОЖНО ВСТРЕЧАЙСЯ В РЕАЛЕ СО СВОИМИ ЗНАКОМЫМИ ИЗ ИНТЕРНЕТА!
5. ЕСЛИ ТЕБЯ ПРЕСЛЕДУЕТ И ОСКОРБЛЯЮТ В ИНТЕРНЕТЕ, ДЕЛАЮТ РАЗНЫЕ НЕПРИСТОЙНЫЕ ПРЕДЛОЖЕНИЯ — НЕ БОЙСЯ СКАЗАТЬ ОБ ЭТОМ СТАРШИМ.
6. НЕ ОБЩАЙСЯ С ТРОЛЛЯМИ — ИНТЕРНЕТ-ХАМАМИ. НЕ ПОРТЬ СЕБЕ НАСТРОЕНИЕ.

Ростелеком

Представить нашу жизнь без Internet, сейчас практически невозможно. И ни для кого не секрет, что социальные сети находятся на пике своего развития. А что они в себе несут – добро или зло – мы считаем, ответ на этот вопрос каждый должен дать себе сам.

Социальные сети – это все-таки польза, если пользоваться ими с умом и в меру!

Спасибо!

Ростелеком