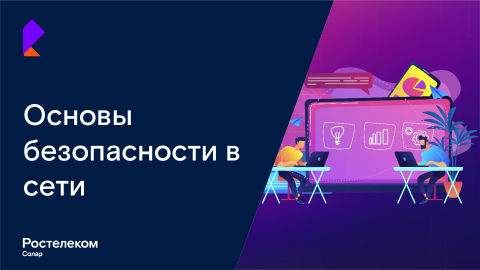
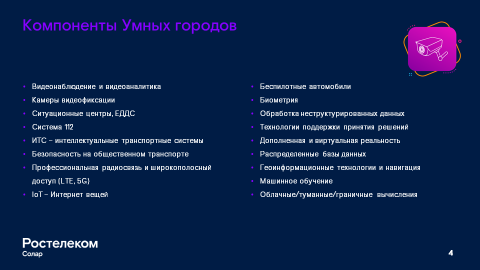
1. Лекция «Основы Кибергигиены»



Дорогие друзья!

Новости о взломах, краже аккаунтов и денег со счетов, к сожалению, стали привычными. Если пенсионеров обманывают с помощью телефонных звонков, то в соцсетях и мессенджерах жертвой может стать любой. Специалисты «Ростелеком», у которого есть целое подразделение по борьбе с киберпреступниками с киберполигонами и огромной командой разработчиков, подготовили базовые правила – как каждый может защититься от злоумышленников. В каждом районе у нас интернет. У каждого из вас телефон и аккаунты в соцсетях. Это самые разные возможности – и к сожалению, не только для вас, но и для злоумышленников.

1. **Умные города (обоснование, определение, составные части)**

****

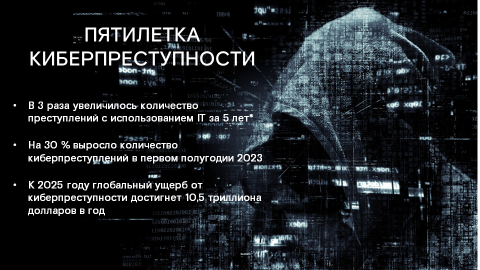
Насколько технологии проникли в нашу жизнь? Буду называть понятия, а вы говорите – знакомы с ними или нет

* **Видеонаблюдение и видеоаналитика**
* **Ситуационные центры**
* **Система 112**
* **Профессиональная радиосвязь и широкополосный доступ (LTE, 5G)**
* **IoT – Интернет вещей**
* **Беспилотные автомобили**
* **Биометрия**
* **Обработка неструктурированных данных**
* **Распределенные базы данных**
* **Геоинформационные технологии и навигация**
* **Облачные/туманные/граничные вычисления**

Пользуется ими и власти, чтобы вести хозяйство, следить за преступностью.

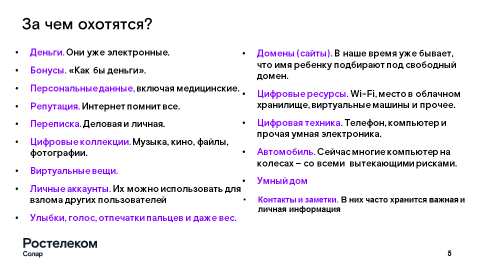
Пользуется ими бизнес – чтобы ваши родители, например, могли получить одобрение на услугу в банке без сбора кучи документов и заявок. Или интернет магазины – чтобы предложить именно те товары, которые вам понравятся, определить по геометке удобный пункт доставки и рассчитать ее время. И многое другое

1. **Масштабы угроз**

****

Посмотрим данные от полиции за этот год. Каждое четвертое преступление в России происходит с использованием интернета. Атакуют людей персонально и компании, госорганизации.

1. **За чем охотятся?**



С компаниями отдельный разговор, но поговорим про каждого из вас персонально. Кто-то скажет – у меня нет миллионов, и красть у меня нечего. Но давайте посмотрим – что можно украсть, а вы про себя считайте, что из списка есть у вас.

**Деньги. Они уже электронные.**

**Бонусы. «Как бы деньги».**

**Персональные данные, включая медицинские.**

**Репутация. Интернет помнит все.**

**Переписка. Деловая и личная.**

**Цифровые коллекции. Музыка, кино, файлы, фотографии.**

**Виртуальные вещи.**

**Личные аккаунты. Их можно использовать для взлома других пользователей**

**Улыбки, голос, отпечатки пальцев и даже вес.**

**Домены (сайты). В наше время уже бывает, что имя ребенку подбирают под свободный домен.**

**Цифровые ресурсы. Wi-Fi, место в облачном хранилище, виртуальные машины и прочее.**

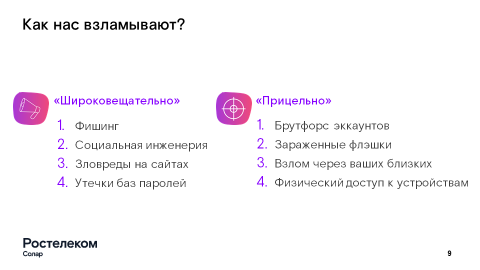
**Цифровая техника.** Телефон, компьютер и прочая умная электроника.

**Автомобиль.** Сейчас многие – это компьютер на колесах – со всеми вытекающими рисками.

**Умный дом**

**Контакты и заметки.** В них часто хранится важная и личная информация

1. **Сценарии кибератак**

****

До недавнего времени были распространены два метода взлома и компрометации цифровых ценностей и ресурсов.

* **Широковещательно** (атаки одновременно на сотни и тысячи пользователей)
* **Прицельно**

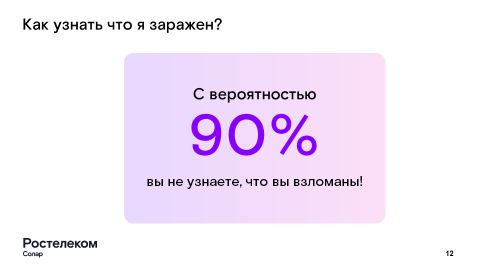
Границы между этими методами были условными, так как для достижения цели у киберкриминала в ход идут все средства. Но затем появился третий сценарий – беспечность!

1. **Как узнать, что ты заражен?**

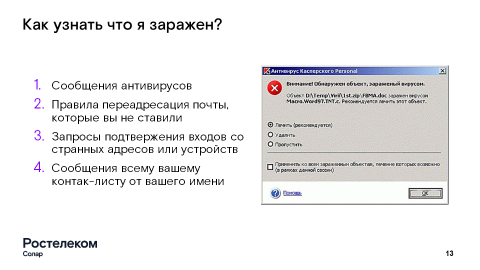


С интересом слушаем ответы. Правильный ответ на следующем слайде!

**12. Никак!**

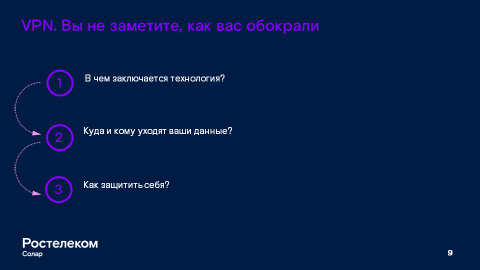


1. Как попасть в 10% тех, кто почуял неладное



Как минимум 4 способа есть

1. **ВПН –что это такое?**



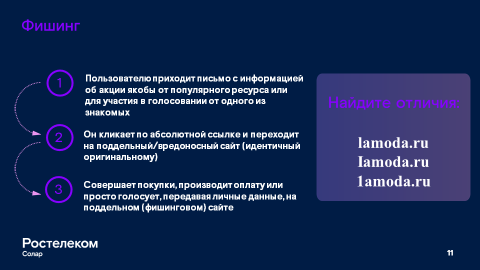
Кто пользуется этими сервисами? Кто может объяснить, что это? Кто из вас скачал их бесплатно просто в магазине приложений?

В таком случае, весьма вероятно, ваши данные уже утекли к злоумышленникам. Пароли от мессенджеров, магазинов, соцсетей.

Что такое ВПН - виртуальная частная сеть — это безопасное зашифрованное подключение пользователя к сети. Вам присваивают виртуальный айпи-адрес, привязанный к серверу в другой стране. Что помогает: зашифровать ваши данные, скрыть геолокацию и обойти локальные ограничения, сохранять конфиденциальность при посещении русурсов в интернете. Если вы покупает себе место на сервере сами и настраиваете сеть – одно дело. Но пользуясь приложением, даже тем, которое уже есть у друга, норм работает, вы всегда рискуете – считай, просто передаете всю информацию, которую отправляете кому-то. Если приложение бесплатное, то нетрудно догадаться, что зарабатывают его создатели на чем-то другом. И скорее всего, способ заработка связан с данными пользователями. Как защититься?

В идеале не использовать, получить свою сеть или сеть работодателя. Но если полезли, не пользуйтесь теми приложениями, где хранятся ваши пароли, данные , которые не хотите просто отдать кому-то.

1. **Фишинг**

****

Рассмотрим еще один способ обмана.

Фишинг. Вид интернет-мошенничества путем проведения массовых рассылок электронных писем, например от имени популярных брендов, а также личных сообщений внутри социальных сетей. Выигрыш, акция или предупреждение о взломе и просьба подтвердить аккаунт или проголосовать за друга – замаскироваться может под любой ресурс

• Пользователю приходит письмо с информацией об акции на таком-то ресурсе или просьбой проголосовать от друга в чате

• Он кликает по абсолютной ссылке и переходит на поддельный сайт (идентичный оригинальному)

Итог – злоумышленники похищают данные карты (если ее там просят ввести) или даже угоняют аккаунт целиком с личными фото, номерами карточек, пинкодами.

Как распознать обман?

Зайти на официальный сайт сервиса, вбив адрес в поисковик, а не просто кликнув на ссылку,

Написать знакомому, приславшему ссылку, в другом мессенджере или позвонить,

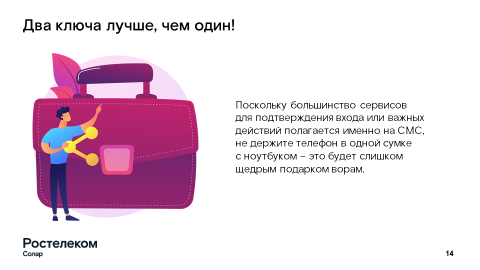
Присмотреться к сайту – все ли буквы на месте, тот ли домен (буквы после точки)

Например, gosuslugi.ru сайт прописан верно, gosuslugi.su адрес до точки тот же, но домен неверный (.su, .org)

Убедиться, что письмо от магазина не с личной почты/популярного сервиса: gosuslugi@mail.ru – с мейла госуслуги слать письмо не будут

Вопрос: где тут настоящий адрес сайта? Ответ: «все написания бренда Lamoda поддельные»

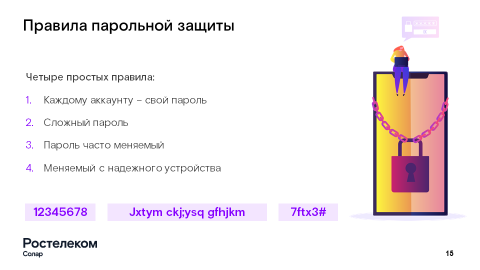
1. **Двухфакторная аутентификация**

****

Двухфакторная аутентификация по смс

Однако есть и минусы – ваш телефон всегда должен быть в зоне действия сети, заряжен и оплачен, иначе СМС к вам не придет.

1. **Правила парольной защиты**



* Каждому эккаунту – свой пароль
* Сложный пароль
* Пароль часто меняем
* Меняем с надежного устройства

Какой из предложенных (на слайде) паролей наиболее стойко защитит наши ресурсы?

Длинные пароли, состоящие из 12 символов и более, ломаются ничуть не хуже, чем короткие, если для их составления люди используют фразы, состоящие из 3-4 обычных слов – такая задача легко решается с помощью перебора по словарю.

Также наивно использовать в качестве пароля русские слова, набранные латиницей. Например, второй «**JxtymCkj;ysqGfhjkm**» на самом деле в русской раскладке клавиатуры будет «ОченьСложныйПароль», что вскрывается программными средствами в два счета.

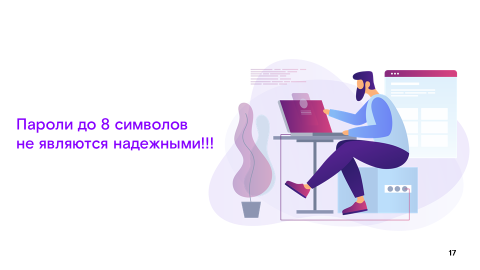
Тогда остается третий вариант **7ftx3#**

Но и у этого пароля есть один недостаток. В нем только 6 символов!

**16. Пароли длиной до 8 символов включительно в общем случае не являются надежными**

Допустим, что в вашем пароле используются 36 различных символов (латинские буквы одного регистра + цифры), а скорость перебора составляет 100 000 паролей в секунду.

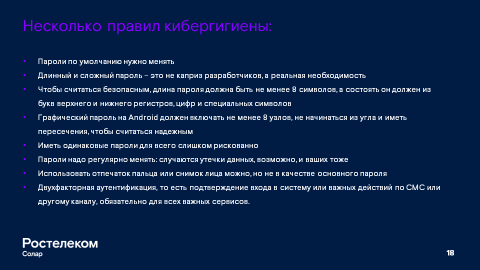
Разница во взломе пароля из 7 и 8 символов составит 9 дней и 11 месяцев соответственно.



Таким образом, **пароли длиной до 8 символов включительно в общем случае не являются надежными.** Для повышения стойкости пароля важна даже не столько его длина, сколько разнообразие используемых символов. Именно поэтому сервисы, которые действительно заботятся о безопасности своих пользователей, требуют, чтобы пароль обязательно содержал буквы верхнего и нижнего регистра, цифры и специальные знаки.

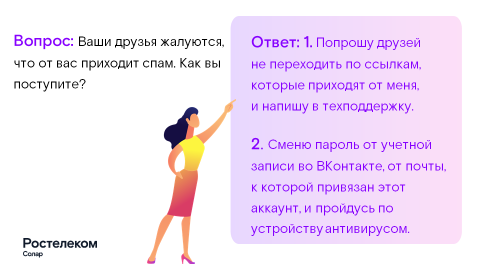
**Эффективность брутфорс-атаки обратно пропорциональна уровню беспечности пользователя. Чем надежнее ваш пароль, тем меньше шансов его взломать в лоб.**

18 . **Главное** — **соблюдать правила кибергигиены. Вот некоторые из них:**



* Пароли, которые предлагают производители устройств или программ, нужно менять до подключения к интернету или при первом подключении
* Пароль не бывает удобным, красивым или модным. Пароль бывает надежным и ненадежным!
* Чтобы считаться безопасным, длина пароля должна быть не менее 8 символов, а состоять он должен из букв верхнего и нижнего регистров, цифр и специальных символов.
* Графический пароль на Android должен включать не менее 8 узлов, не начинаться из угла и иметь пересечения, чтобы считаться надежным.
* Иметь одинаковые пароли для всего слишком рискованно. По крайней мере для всех важных сервисов пароли должны быть уникальными.
* Пароли надо регулярно менять: случаются утечки данных, возможно, и ваших тоже, и вы о них не узнаете
* Использовать отпечаток пальца или снимок лица можно, но не в качестве основного пароля.
* Двухфакторная аутентификация, то есть подтверждение входа в систему или важных действий по СМС или другому каналу, обязательна для всех важных сервисов.

**20. Контрольные вопросы**

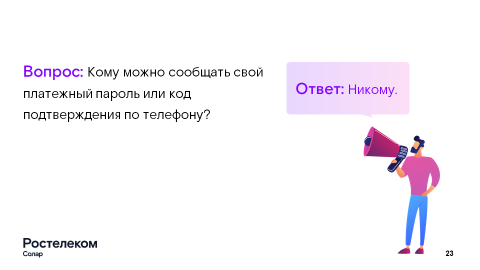
****

**Ваши друзья жалуются, что от вас приходит спам. Как вы поступите?**

**Ответы:**

1. Попрошу друзей не переходить по ссылкам, которые приходят от меня, и напишу в техподдержку
2. Сменю пароль от учетной записи во ВКонтакте, от почты, к которой привязан этот аккаунт, и пройдусь по устройству антивирусом

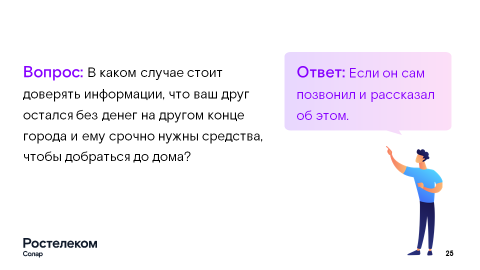
**23-24**



**Вопрос:** Кому можно сообщать свой платежный пароль или код подтверждения по телефону?

**Ответ:** Никому

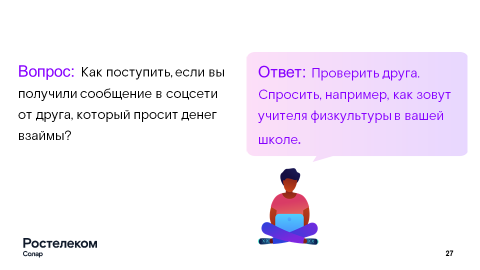
**25-26:**



**Вопрос:** В каком случае стоит доверять информации, что ваш друг остался без денег на другом конце города и ему срочно нужны средства, чтобы добраться до дома?

**Ответ:** Если он сам позвонил и рассказал об этом.

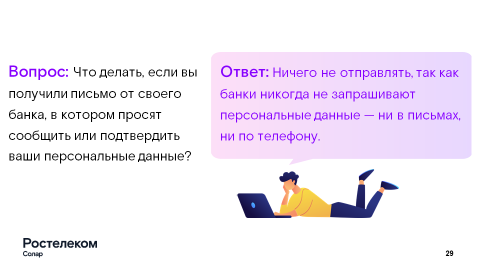
**27-28:**



**Вопрос:** Как поступить, если вы получили сообщение в соцсети от друга, который просит денег взаймы?

**Ответ:** Проверить друга — спросить, например, как зовут учителя физкультуры в вашей школе.

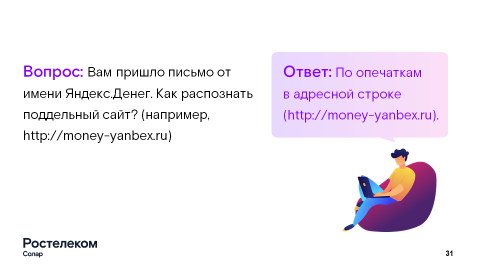
**29-30:**

****

**Вопрос**: Что делать, если вы получили письмо от своего банка, в котором просят сообщить или подтвердить ваши персональные данные?

**Ответ:** Ничего не отправлять, так как банки никогда не запрашивают персональные данные — ни в письмах, ни по телефону.

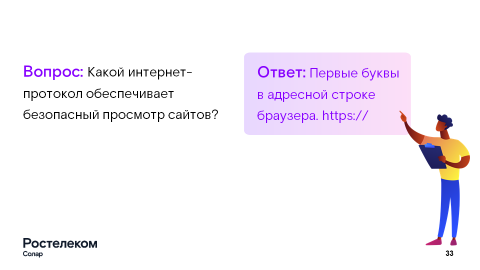
**31-32:**

****

**Вопрос:** Вам пришло письмо от имени Яндекс.Денег. Как распознать поддельный сайт? (например, <http://money-yanbex.ru>)

**Ответ:** По опечаткам в адресной строке (<http://money-yanbex.ru>)

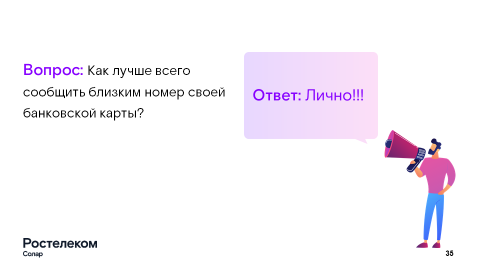
**33-34:**

****

**Вопрос:** Какой интернет-протокол обеспечивает безопасный просмотр сайтов?

**Ответ:** Первые буквы в адресной строке браузера. https://

**35-36:**



**Вопрос:** Как лучше всего сообщить близким номер своей банковской карты?

**Ответ:** Лично

**37. Если вы в себе уверены и готовы пройти проверку самостоятельно – попытайте удачу в нашем тесте. Каждый из вас получит сертификат**

**Кроме того, до 30 сентября можно принять участие в розыгрыше – условия будут размещены в группе** Управления образования и науки в ВК (под этим постом нужно будет разместить СКРИН С РЕЗУЛЬТАТАМИ ТЕСТА \*)

Ну а тем, кого тема заинтересовала, мы дарим бесплатный доступ к книге о киберпреступлениях и защите от них

