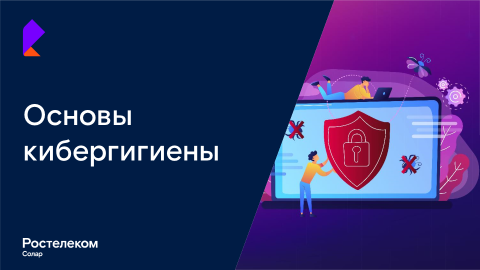
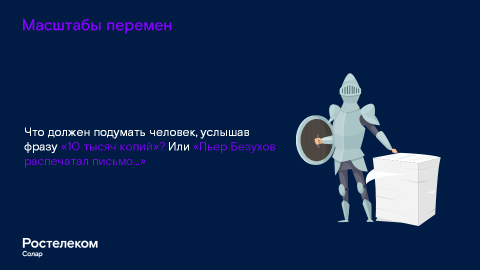
1. Лекция «Основы Кибергигиены»



1. **Масштабы перемен современного мира (10 тыс. копий)**

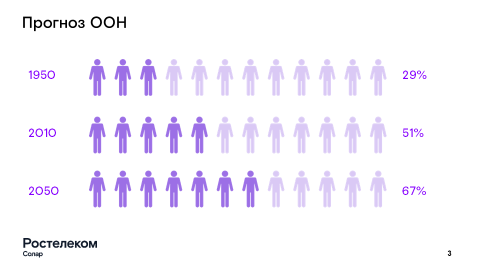
****

Что представляет себе современный человек, услышав фразу «10 тысяч копий»? Как правило все, что угодно, но не армию Александра Македонского. А где в романе «Война и Мир» после фразы «Пьер Безухов распечатал письмо…» искать принтер?

Мир вовсе не сходит с ума, как кто-то может решить. Дело в том, что наш мозг ничем не отличается от мозга людей, живших 200 лет назад. Современный мир меняется быстрее, чем за ним поспевает эволюция. Технологии ускорили время и сделали человека еще сильнее. Но готовы ли мы к этим переменам, когда инструменты управления, которые мы использовали пять или десять лет назад, больше не работают?

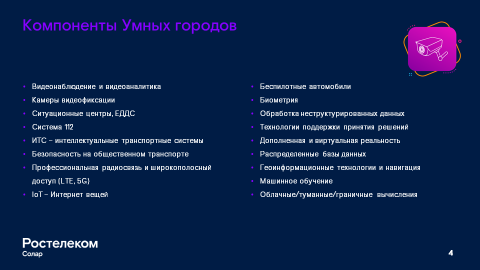
Каждое поколение считает, что их устойчивость к переменам выше, чем у их родителей. Это верно, но только от части. Дело в том, что в своих прогнозах и ожиданиях перемен стало появляться много ошибок. Перемены наступают гораздо быстрее, чем их прогнозируют и одинаково накрывают всех.

1. **Прогноз ООН**

****

По оценкам Организации Объединенных Наций, к 2050 году 67% населения Земли будут проживать в городах. Уже сейчас некоторые мегаполисы мира перенаселены. Муниципалитеты не всегда справляются с уборкой мусора, в некоторых районах перебои с электричеством случаются чаще, чем в других, и так далее. Чтобы повысить качество городских услуг, администрации все чаще внедряют различные информационные системы.

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

****

«Умный город» (или smart city) — это не просто модная концепция. Правда, понять, что именно представляет собой «умный город» и почему он «умный», не всегда просто. Как отличить город, который уже «умный», от того, который еще не поумнел?

Полвека назад жизнь в городах текла относительно неспешно, что позволяло коммунальным и другим службам поддерживать в них чистоту и порядок. Но в конце XX века ситуация сильно изменилась. Рост городского населения привел к транспортным коллапсам, многократно возросла нагрузка на жилищно-коммунальные службы. Годами работавшие алгоритмы городского хозяйства стали давать сбои. Когда-то полупустые улицы начали задыхаться в автомобильных пробках. Росли очереди в поликлиниках и государственных организациях, работающих с населением. Все попытки оптимизировать работу ведомств и отдельных чиновников приносили мало пользы. Увеличение штата работников служб тоже ни к чему не привело.

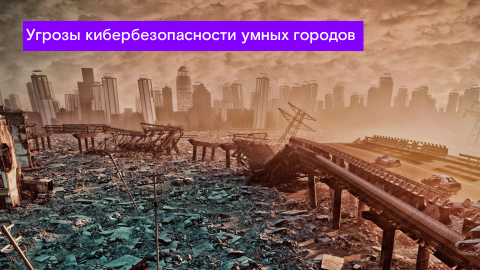
Вывод: городскому хозяйству требуются решения, позволяющие перенести большую часть управленческой нагрузки на компьютеры, которые, как известно, не устают и почти не ошибаются, то есть сделать городское хозяйство максимально автоматизированным, а город — «умным».

Под престижной маркой «умного города» властные структуры в большинстве стран мира пытались продвигать прежде всего «город богачей» или «город предпринимателей». Все инфраструктурные решения ориентированы были главным образом на обслуживание богатого, мобильного и креативного бизнесмена. Но города — это не просто провода и кабели, умные офисы, модные бары и роскошные отели. Города — это люди, которые заслуживают большего.

Ярлык «умный город» может служить лишь идеологической маской, стремящейся скрыть основные негативные изменения в городах и даже мешать истинному прогрессу. Однако единого определения, что же такое «умный город», не удалось выработать и по сей день.

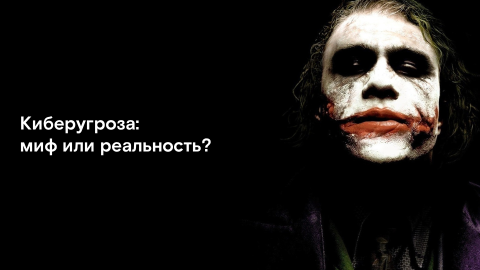
**Но несомненно одно — умному городу должны соответствовать умные люди, которым предстоит всем этим пользоваться и управлять!**

1. **Угрозы безопасности умных городов**



С самого начала эксперты в области безопасности понимали, насколько важно минимизировать риски при функционировании умных городов. Концепция «умного города» широко обсуждается не первый год, множество экспертов работают над созданием особых технологий, которые сделают город энергоэффективным, комфортным, экологичным и физически безопасным. К сожалению, проблемы информационной безопасности таких городов остаются по-прежнему актуальными. Если не подумать о защите заблаговременно, то впоследствии решать возможные проблемы будет гораздо сложнее и затратнее, а город при этом может стать открытым и беззащитным для киберпреступников.

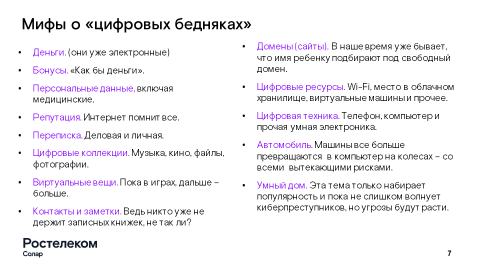
1. **Киберугрозы**



Истории о серьезных компьютерных атаках давно перекочевали из фильмов в повседневные новостные выпуски. И хотя киберпреступления происходят в виртуальном пространстве, их жертвы теряют вполне реальные ценности: персональные данные, деньги, репутацию, а иногда подвергают опасности свое здоровье и жизни.

Все это может произойти, когда человек просто сидит перед компьютером или вводит куда-то свои данные. Сегодняшняя элита преступного мира — это не люди, с криками врывающиеся в банки, а те, кто сидит перед компьютером и совершенно спокойно крадет миллионы. Для современных молодых людей компьютер — это такая же техника, как и любой другой атрибут современного мира. Поэтому киберпространство — одна из главных опасностей этого мира. Однако, это вовсе не значит, что современные технологии нужно запрещать или ограничивать. Потому что не технологии совершают преступления, а люди! Но для того, чтобы не стать жертвой, нужно соблюдать определенные правила кибергигиены. Это одно из необходимых качеств, без которого будет очень сложно соответствовать высоким темпам обмена информацией. А без этого XXI век уже немыслим.

1. **Мифы о «цифровых бедняках»**



Кто-то все еще сомневается, что он в опасности?

Многие считают себя «цифровыми бедняками» – мол, красть у нас нечего, потому и замки не нужны. Когда человек не осознает, что у него есть что-то ценное, любые меры предосторожности кажутся ему избыточными. Скорее всего, в ответ на ваши советы он покрутит пальцем у виска и назовет вас параноиком. В реальной жизни ведь никто не ставит сверхзащищенную железную дверь, когда в доме шаром покати – вот если привалит богатство, тогда об этом и подумаем.

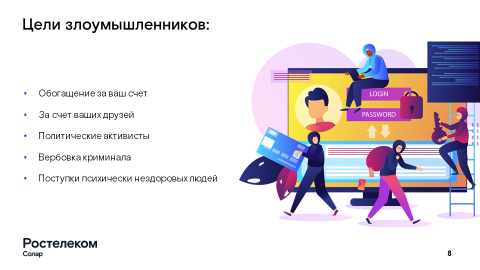
Вполне рациональная точка зрения – ведь стоимость и сложность системы защиты должна быть соразмерна ценности того, что мы пытаемся с ее помощью защитить. Однако в том, что касается цифровых ценностей, наш житейский опыт не всегда является хорошим советчиком – слишком внезапно произошли изменения. Поэтому даже многие взрослые и опытные во всех отношениях люди часто попадают впросак, когда сталкиваются с киберпреступниками или сами случайно уничтожают что-то для себя ценное.

Прежде всего давайте проведем инвентаризацию наших цифровых активов и поймем, чего они на самом деле стоят, а уж потом подумаем, как их защищать от возможных посягательств преступников и собственной неосторожности.

* **Деньги.** Кроме наличных в кошельке они все электронные.
* **Бонусы.** «Как бы деньги» – мили, баллы лояльности и прочее.
* **Персональные данные**, включая медицинские. Пока это просто информация, но в плохих руках она может привести к краже вашей цифровой личности.
* **Аккаунты в соцсетях, страницы и каналы.** Иногда это очень дорогой актив.
* **Цифровые авторские права** на сайты, блоги, фото, видео и другой контент.
* **Тайна частной жизни**. Когда вокруг камеры и микрофоны, это становится роскошью.
* **Репутация**. Интернет помнит все, что написано о вас и все, что вы написали сами.
* **Переписка.** Деловая и личная, в электронной почте и мессенджерах.
* **Цифровые коллекции.** Музыка, кино, файлы, фотографии. Разумеется, без пиратских копий.
* **Виртуальные вещи**. Пока в играх, дальше – больше.
* **Контакты и заметки**. Ведь никто уже не держит записных книжек, не так ли?
* **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.** Машины все больше превращаются в компьютер на колесах – со всеми вытекающими рисками.
* **Умный дом**. Эта тема только набирает популярность и пока не слишком волнует киберпреступников, но угрозы будут расти.

Ого, сколько всего у нас есть ценного! Естественно, найдутся люди, которые захотят это украсть или уничтожить.

1. **Не обязательно быть целью, чтобы стать жертвой**



«У меня нет миллионов в банке, заводов и яхт, в политику я не лезу, — разве я чем-то интересен киберпреступникам?».

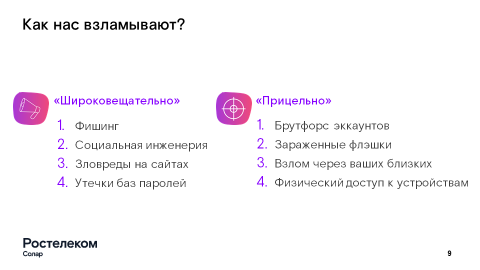
Действительно, преступная деятельность, как и всякая другая, требует организованных усилий зачастую большой группы очень квалифицированных людей, и это стоит дорого. Вспомните любой фильм про ограбление: сколько сил и энергии тратят герои, чтобы завладеть чьими-то сокровищами.

Возможно, лично вы киберпреступникам неинтересны. Но цифровой мир устроен иначе. Здесь можно автоматизировать не только полезные процессы типа госуслуг по записи ребенка в школу или в поликлинику — процесс ограбления тоже можно автоматизировать, и ваши деньги и персональные данные украдут вместе с миллионами других, просто за компанию. Или заразят ваш компьютер или смартфон, и он станет частью преступной сети, атакующей объекты городской инфраструктуры.

**Не обязательно быть целью, чтобы стать жертвой**

Чтобы не попасть в киберкриминальные сети и не стать участником преступных планов, нужно соблюдать хотя бы элементарные правила цифровой гигиены.

1. **Сценарии кибератак**

****

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

* **Широковещательно** или методом брутфорса (по-английски bruteforce – буквально «грубая сила»), основанного на переборе всех возможных значений. Например, если у вас есть чемодан с кодовым замком на 3 цифры от 0 до 9, для его открытия нужно перебрать всего тысячу комбинаций – с этим справится даже ребенок.
* **Прицельно**, (таргетированные или целенаправленные атаки APT (advanced persistent threat)). Когда злоумышленник или группа злоумышленников целенаправленно атакуют конкретные информационные ресурсы.

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. **Беспечность!**

****

* **Беспечность**! Это когда мы сами раскрывает конфиденциальную информацию или не защищаем ее надлежащим образом. А этим всегда готовы воспользоваться злоумышленники.

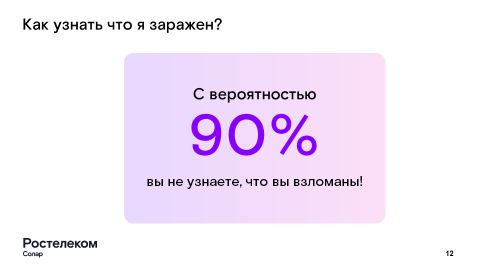
Цифровой мир создал иллюзию простоты. Не только детям, но и взрослым кажется, что все в мире стало просто. Дети верят, что в жизни как в игре можно начать играть заново, а потому спешат «перейти на новый игровой уровень» – повзрослеть. Взрослые быстро находят информацию в интернете, ориентируются по навигаторам, переводят иностранные тексты и начинают верить, что они выучили иностранные языки. Мы привыкли решать проблемы в два клика, так как в три нам кажется уже неудобно. И эти привычки не только создают иллюзию, но и порождают беспечность.

1. **Как узнать, что ты заражен?**

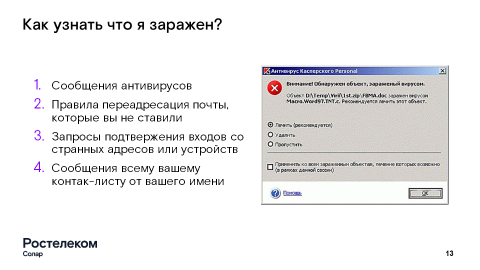


С интересом слушаем ответы. Правильный ответ на следующем слайде!

**12. Никак!**

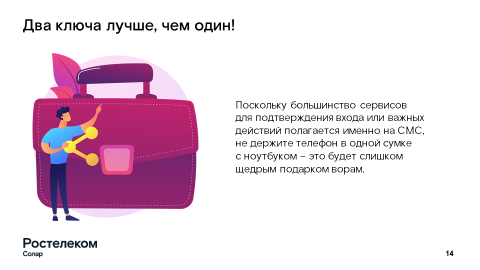


1. Но если никак, то что же делать?



Кибербезопасность — это в первую очередь человеческая, а не техническая проблема. Иногда это утверждение звучит как «человек — самое слабое звено». Хотя люди время от времени совершают ошибки, забывают флешки, не блокируют компьютер, выходя в другую комнату, открывают письма с вредоносными вложениями. Что же делать? Где начинается КИБЕРГИГИЕНА?

**14. Два ключа лучше, чем один**

****

Наверное, у многих на двери в квартиру стоит два замка – для большей надежности. Точно так же и в компьютерных системах: чтобы впустить пользователя часто кроме пароля используется еще и второй параметр. Но не второй пароль! Если злоумышленники как-то узнали один пароль, возможно, они заполучили всю базу или смогли внедриться в систему и перехватывают информацию. Или кто-то украл ваш ноутбук вместе со всеми паролями. В таких случаях специалисты говорят, что канал скомпрометирован.

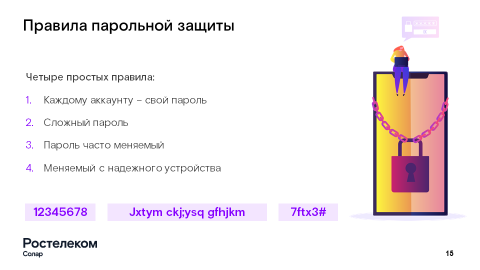
Поэтому нужен другой независимый канал, по которому можно подтвердить, что вы – это вы. Чаще всего в роли второго канала используется СМС – вам на телефон приходит код, который надо ввести в специальное поле для подтверждения входа в систему или совершения каких-то действий. Обычно подтверждение нужно, чтобы перевести деньги или изменить какие-то важные данные.

Эти каналы должны быть принципиально разными. Парольная защита основывается на знании ключа. В принципе, знанием может обладать кто угодно – просто тот, кто украл или получил пароль. Тогда в игру вступает второй фактор, который основан на владении чем-либо, чаще всего телефоном или USB-ключом. Конечно, эту вещь тоже можно украсть, но маловероятно, что одновременно с паролем.

**Кстати, поскольку пока большинство сервисов для подтверждения входа или важных действий полагается именно на СМС, не держите телефон в одной сумке с ноутбуком – это будет слишком щедрым подарком ворам.**

Однако есть и минусы – ваш телефон всегда должен быть в зоне действия сети, заряжен и оплачен, иначе СМС к вам не придет. К тому же для многих смартфон стал сегодня основным или даже единственным средством доступа в интернет, поэтому фактически происходит слияние двух факторов в один – если кто-то завладел вашим телефоном, он с него войдет в ваш аккаунт и на него же получит код. Так что плюс оборачивается минусом.

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, «**JxtymCkj;ysqGfhjkm**» на самом деле в русской раскладке клавиатуры будет «ОченьСложныйПароль», что вскрывается программными средствами в два счета.

Тогда остается третий вариант **7ftx3#**

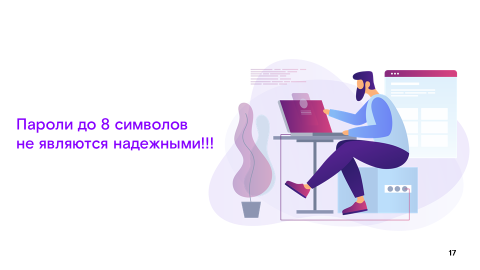
Но и у этого пароля есть один недостаток. В нем только 6 символов!

**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.

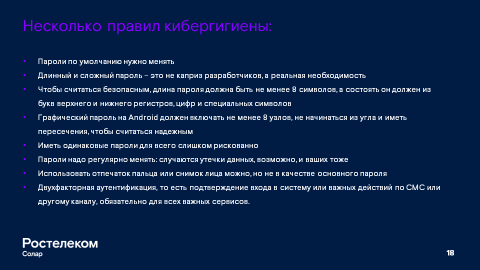


Таким образом, **пароли длиной до 8 символов включительно в общем случае не являются надежными.** Для современных компьютеров этот показатель гораздо выше. Так, 64-битный ключ (пароль) подбирается на современном компьютере примерно за два года, но перебор легко может быть распределен между множеством компьютеров.

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.

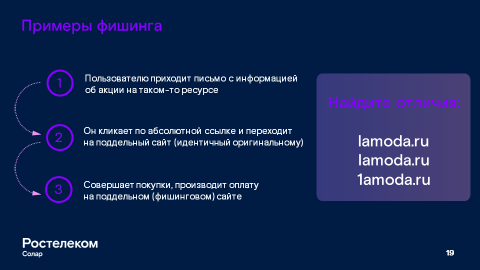
**Эффективность брутфорс-атаки обратно пропорциональна уровню беспечности пользователя. Чем надежнее ваш пароль, тем меньше шансов его взломать в лоб.**

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!
* Длинный и сложный пароль — это не каприз разработчиков, а реальная необходимость. 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.
* 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.

**19. Фишинг**



Рассмотрим еще один способ обмана.

**Фишинг.** Вид интернет-мошенничества путем проведения массовых рассылок [электронных писем](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0), например от имени популярных брендов, а также личных сообщений внутри социальных сетей.

Люди часто открывают вложения в письмах или кликают по ссылкам, что приводит к установке шпионских программ. Хакеры стали куда умней и при рассылке фишинговых писем используют информацию из социальных и профессиональных сетей, поэтому получателям все труднее отличить эти послания от обычных писем.

В письме часто содержится прямая ссылка на сайт, внешне похожий на настоящий. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на ней свои логин и пароль, которые он использует для доступа к определенному сайту. Это позволяет мошенникам получить доступ к аккаунтам и банковским счетам. Расчет на то, что многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее!

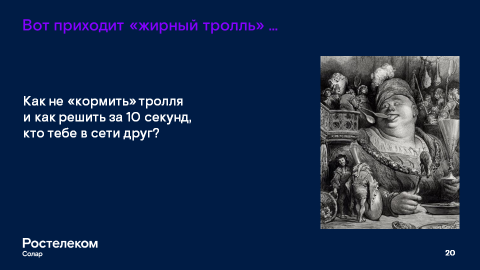
Пример. Вы получаете электронное письмо от сайта Госуслуги с просьбой под каким то предлогом зайти на сайт и ввести свой логин и пароль. Тут же – удобная ссылка, похожая на настоящую (например, отличается на одну букву). Вы переходите по ссылке и видите сайт, один в один похожий на сайт государственных услуг – но на самом деле это подделка. Вы вводите логин и пароль на подконтрольном злоумышленнику интернет-ресурсе и таким образом сами передаете ему свои учетные данные от сайта.

Тщательно проверяйте все ссылки, особенно из плохо известных вам источников. Можно скопировать ссылку или ввести ее в поисковик, скорее всего браузер сам исправит опечатку и выдаст вам уже корректную ссылку.

Ответ на вопрос: «все написания бренда **Lamoda** поддельные»

**20. Социальные сети**

Или как решить за 10 секунд, кто тебе в сети друг



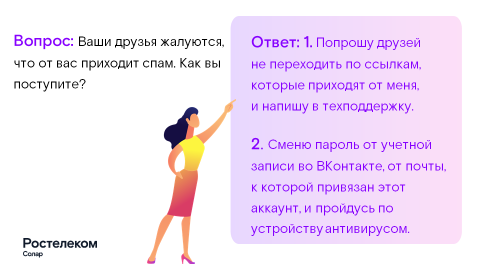
«Властью, данной мне Инстаграмом, объявляю себя моделью!»

О да, нынче моделей у нас треть страны. И все бы ничего, порой даже мило. Главное – не перегибать палку. Ведь за виртуальным имиджем сегодня надо тщательно следить. Соблюдение общих правил этики в сетевом общении так же важно, как и в реальной жизни. Наши манеры – это то, на чем строится имидж и представление о человеке. Но сетевое общение стерло привычные границы. В интернете мы можем легко общаться с людьми другой национальности, расы, вероисповедания. Важно помнить, что тактичный человек никогда не будет делать неуместные акценты на этих особенностях, равно как и без надобности затрагивать потенциально острые темы: политику, неприемлемость религиозных взглядов и пр. В целом правила общения в социальных сетях подобны обычным правилам общения в общественном месте или на улице. Однако многие пользователи из-за особенностей общения в интернете забывают об элементарных правилах хорошего тона и личной безопасности.

Если к вам пришел в ленту соцсети странный гость (например «жирный тролль»), то не пытайтесь с ним спорить или отвечать. Не кормите тролля. Игнорируйте. И он сам потеряет к вам интерес, после чего его можно заблокировать. Напишите в личных сообщениях друзьям, чтобы все его не замечали. Тем самым вы не оставите их наедине с хамством незваного гостя.

Но что делать, если к вам просятся в друзья? Под маской аватарки может скрываться кто угодно, и тут нужно не забывать, что это цифровой мир является продолжением нашей реальной жизни, а не наоборот. Добавлять в друзей лучше всего тех, с кем вы уже знакомы в реальной жизни. Впрочем, бывают и исключения. Тогда многое о человеке расскажет его манера высказывать свое мнение в сети. Даже самые интересные мысли и факты в хамском формате могут оказаться неуслышанными и непонятыми. Во-вторых, важно внимательно смотреть на содержание сообщений – так ли они интересны и важны? И только на третьем месте, кто этот человек. Людой авторитет нуждается в подтверждении и обновлении! И на 10 секунде у вас останется время, чтобы спросить себя «а так ли важен мне этот виртуальный друг?»

**20. Контрольные вопросы**

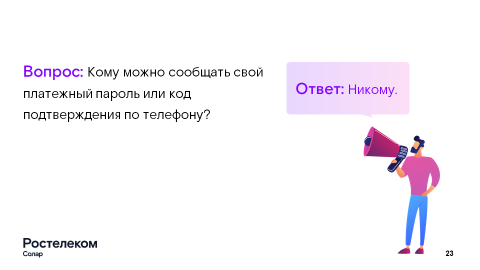
****

**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

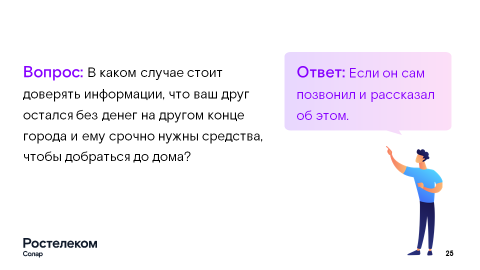
**23-24**



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

**Ответ:** Никому

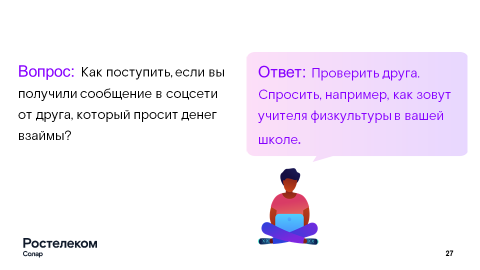
**25-26:**



**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.

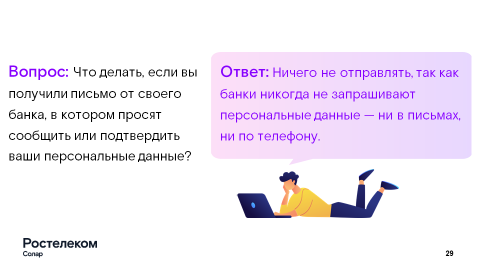
**27-28:**



**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.

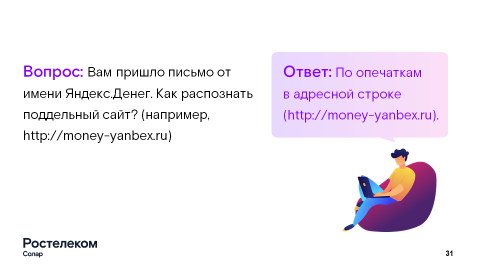
**29-30:**

****

**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.

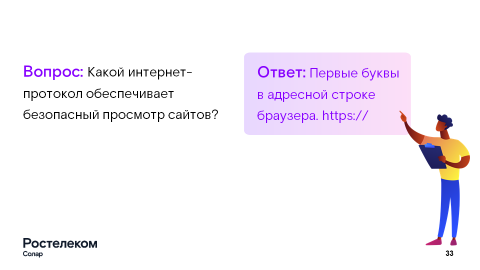
**31-32:**

****

**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>)

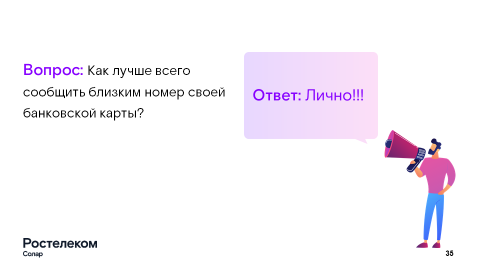
**33-34:**

****

**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. Контакты**

