Цифровая гигиена. Семь кейс-технологий

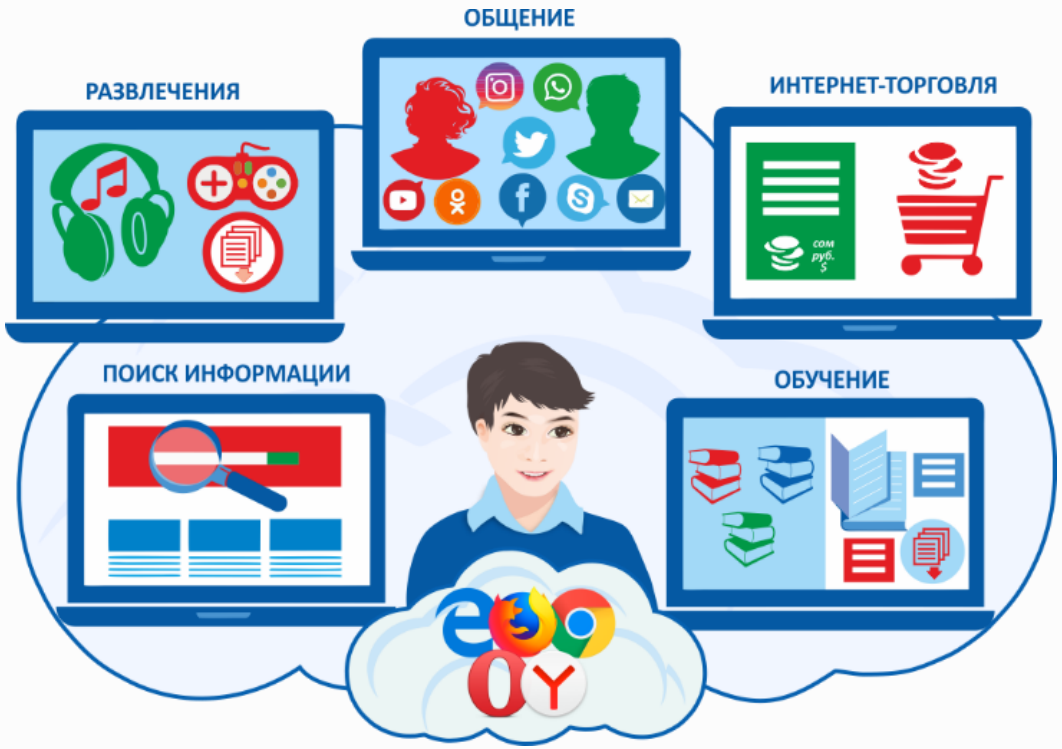
ГБОУ СОШ «Оц» с. Богатое 8Г

Содержание

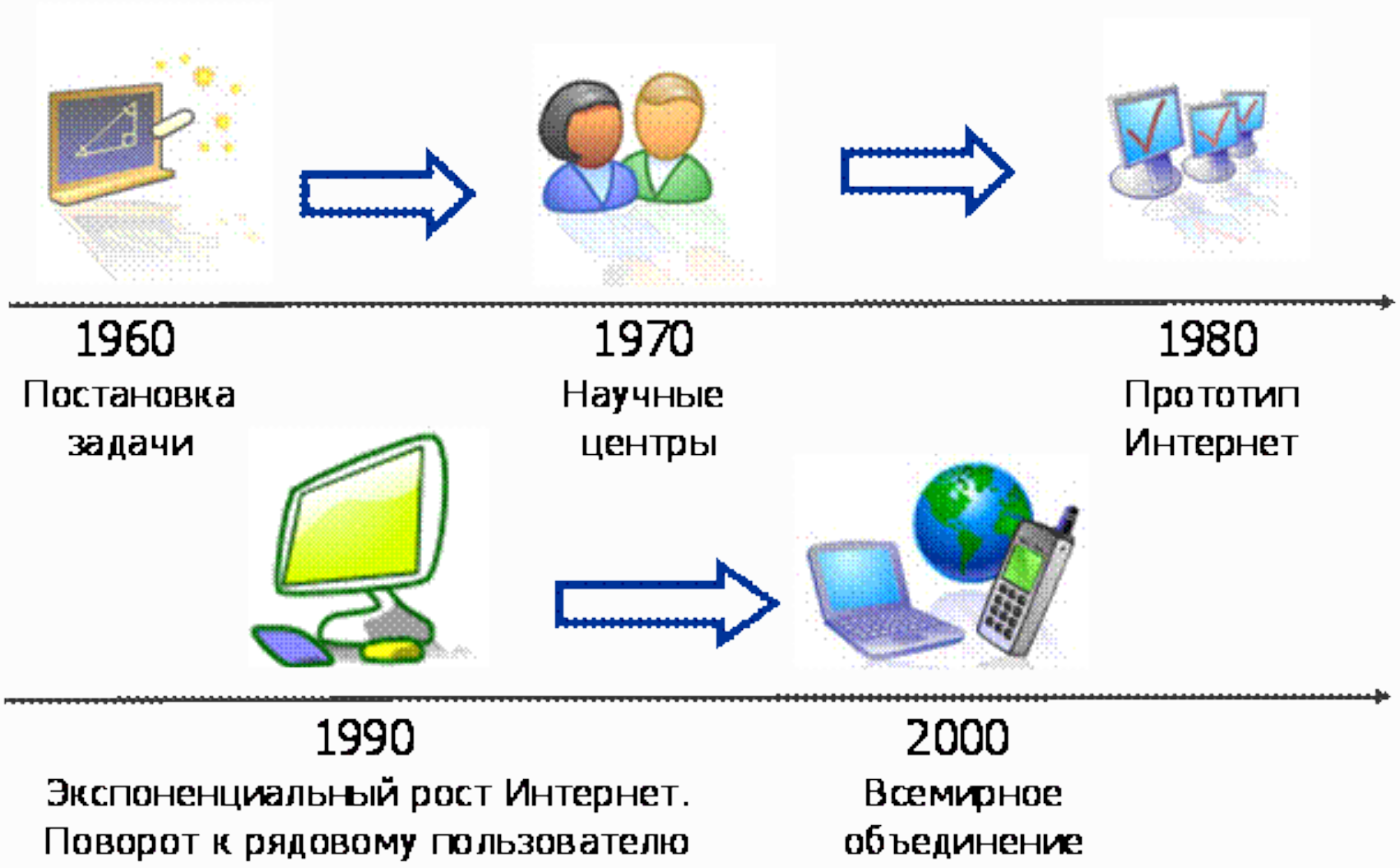
1. История возникновения Интернета.
2. Понятия Интернет - угроз.
3. Изменения границ допустимого в контексте цифрового образа жизни.
4. Изменения нормативных моделей развития и здоровья детей и подростков.
5. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности.
6. Обеспечение эмоционально - психологического периметра безопасности в соответствии с возрастными особенностями ребенка.
7. Баланс ценностей развития и ценностей безопасности.
8. Обращение с деньгами в сети Интернет

История возникновения Интернета

Интернет является основой сети (the Web), технической инфраструктурой, благодаря которой и существует Всемирная Паутина. По своей сути, интернет - очень большая сеть компьютеров, которые могут взаимодействовать друг с другом.



История возникновения Интернета



Понятие Интернет - угрозы

Интернет – это безграничный мир информации, который дает широкие возможности для общения, обучения, организации работы и отдыха и в то же время представляет собой огромную, ежедневно пополняющуюся базу данных, которая содержит интересную для злоумышленников информацию о пользователях.

Угроза – это потенциально возможное событие, действие, которое посредством воздействия на объект защиты может привести к нанесению ущерба.

Существует два основных вида угроз, которым могут подвергаться пользователи: **технические** и **социальная инженерия**.

Технические угрозы

Основными техническими угрозами для пользователей являются **вредоносные программы, ботнеты, DoS и DDoS-атаки**.

Вредоносные программы

Цель вредоносных программ – причинить ущерб компьютеру, серверу или компьютерной сети. К вредоносным программам относятся вирусы, черви, троянские программы.

Вирус – разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликации) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы.

Черви – это разновидность вирусов. Они полностью оправдывают свое название, поскольку распространяются путем «переползания» из устройства в устройство.

Троянские программы – вредоносные программы, которые целенаправленно внедряются злоумышленниками для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Технические угрозы

Основными техническими угрозами для пользователей являются **вредоносные программы, ботнеты, DoS и DDoS-атаки**.

Ботнеты

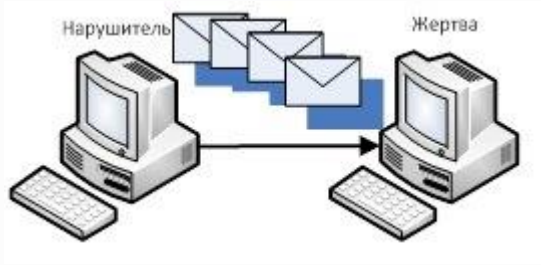
Злоумышленники могут заражать компьютер, чтобы сделать его частью ботнета – сети из зараженных устройств, расположенных по всему миру. Крупные ботнеты могут включать в себя десятки и сотни тысяч компьютеров. Пользователи часто даже не догадываются, что их компьютеры заражены вредоносными программами и используются злоумышленниками. Ботнеты создаются путем рассылки разными способами вредоносных программ, а зараженные машины в дальнейшем регулярно получают команды от администратора ботнета, так что оказывается возможным организовать согласованные действия компьютеров-ботов по атаке других устройств и ресурсов.

Технические угрозы

Основными техническими угрозами для пользователей являются **вредоносные программы, ботнеты, DoS и DDoS-атаки**.

DoS и DDoS атаки

DoS-атака (отказ в обслуживании) – это атака, приводящая к парализации работы сервера или персонального компьютера вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс.



DDoS-атака (распределенный отказ в обслуживании) – это разновидность DoS-атаки, которая организуется при помощи очень большого числа компьютеров, благодаря чему атаке могут быть подвержены сервера даже с очень большой пропускной способностью Интернет-каналов.

Социальная инженерия

Этот сложный термин обозначает способ получать нужную информацию не с помощью технических возможностей, а путем обыкновенного обмана, хитрости. Социальные инженеры применяют психологические методы воздействия на людей через электронную почту, социальные сети и службы мгновенного обмена сообщениями. В результате их умелой работы пользователи добровольно выдают свои данные, не всегда понимая, что их обманули.

Фишинг является наиболее популярным способом атаки на пользователей и одним из методов социальной инженерии. Он представляет собой особый вид Интернет-мошенничества. Цель фишинга – получение доступа к конфиденциальным данным, таким как адрес, телефон, номера кредитных карт, логины и пароли, путем использования поддельных веб-страниц.

Цифровая гигиена

Цифровая гигиена - это набор простых правил, которые позволяют безопасно пользоваться электронной почтой, различными сайтами и соцсетями.

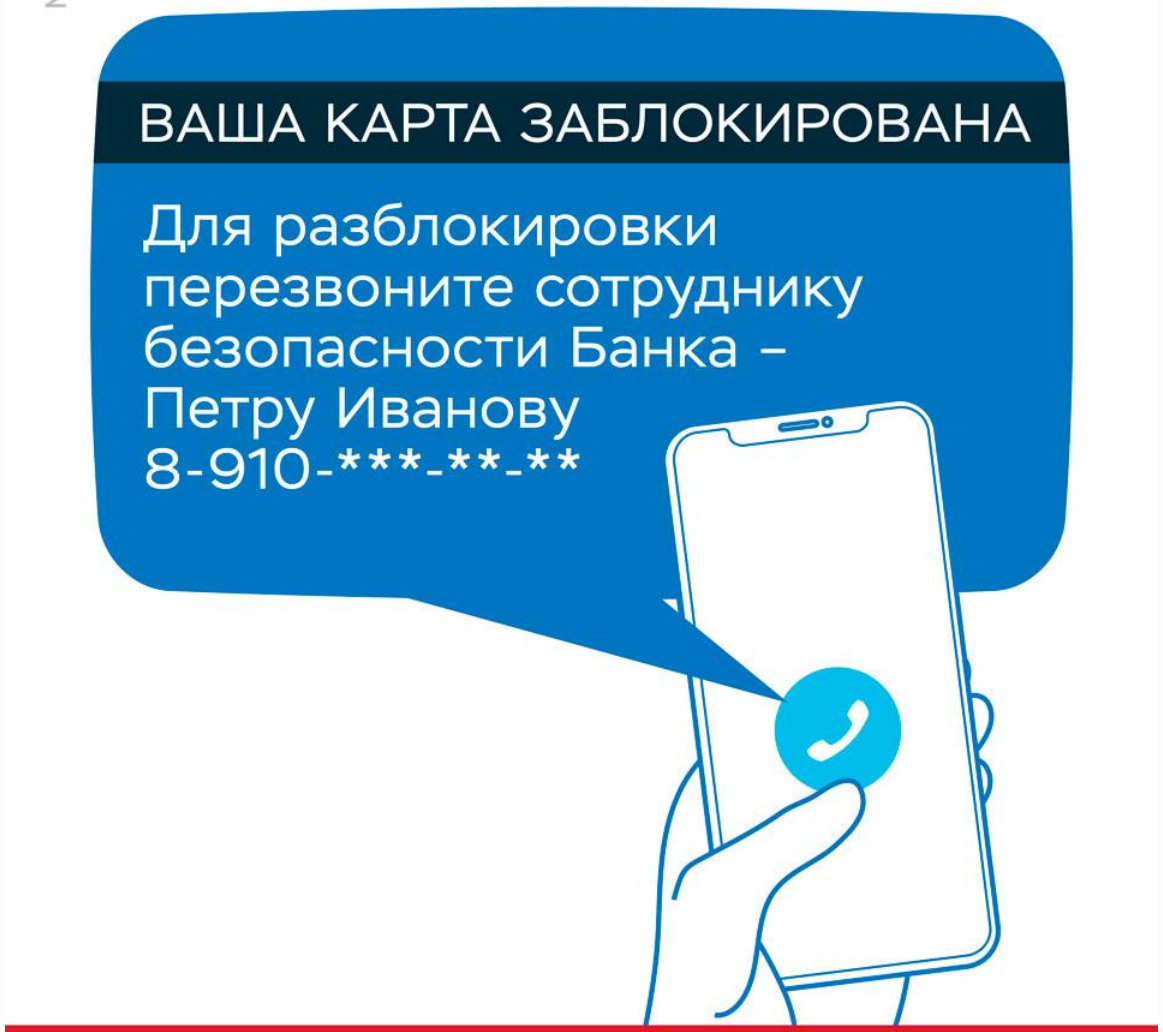
- **ЦИФРОВАЯ ГИГИЕНА**

1. *неол.* свод указаний о наилучших способах сохранения информационной безопасности цифрового устройства и содержащихся на нём данных ◆ Но все же обычным гражданам не повредит соблюдать **цифровую гигиену**: регулярно менять пароли, шифровать сообщения, не открывать незнакомые ссылки.

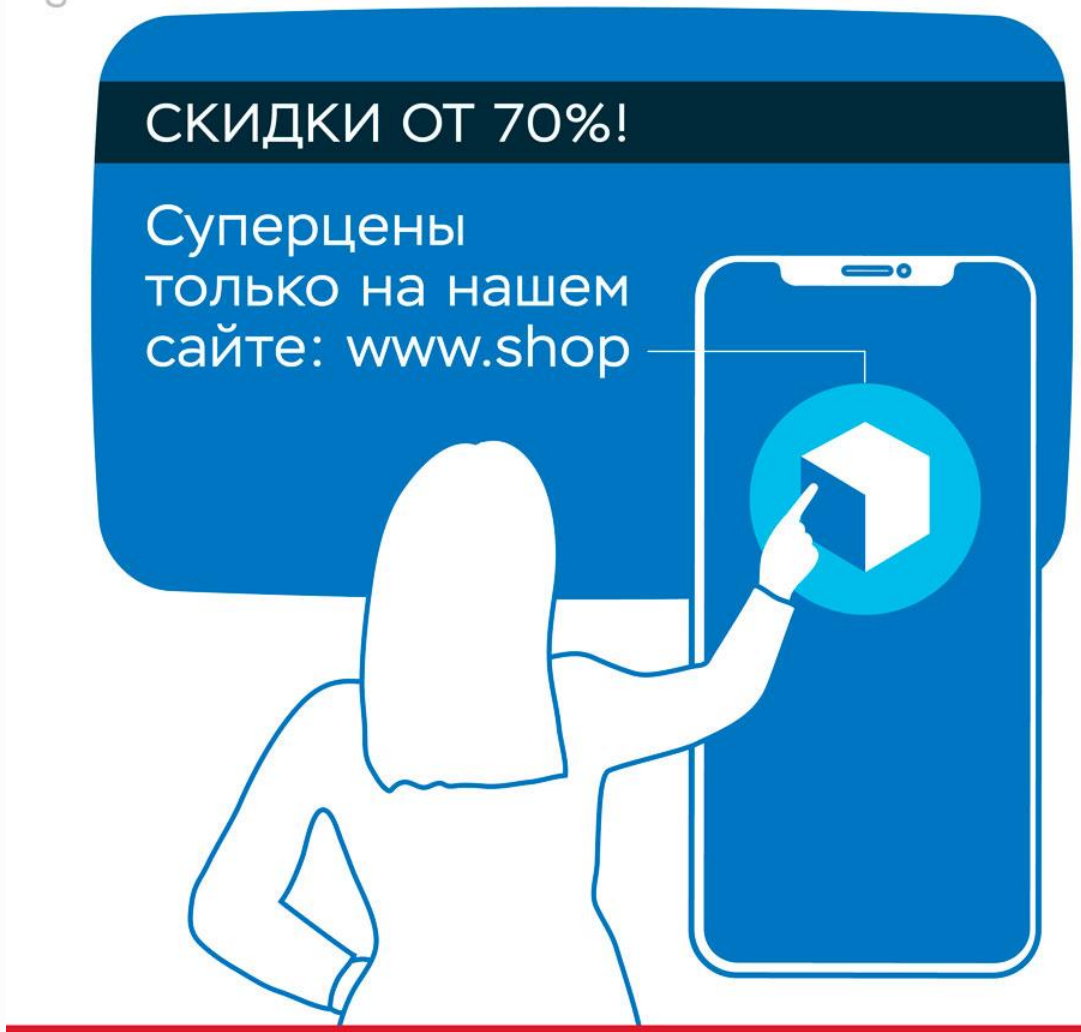
2. *неол.* *разг.* совокупность влияющих на информационную безопасность действий, совершаемых определённым человеком

Цифровая гигиена. Правила

2

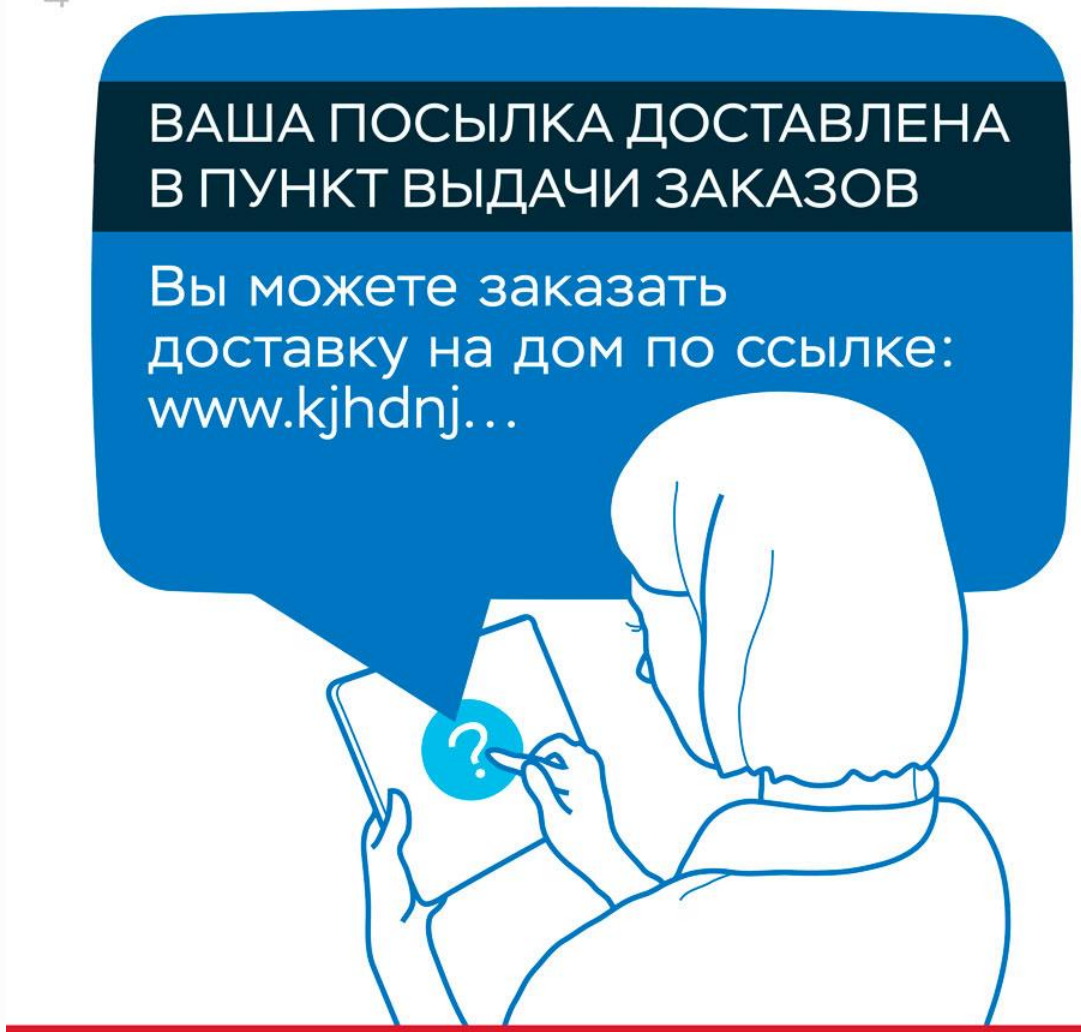


Цифровая гигиена. Правила



«Выгодные предложения» могут оказаться уловкой. С их помощью мошенники завлекают пользователей в свои фальшивые интернет-магазины. Это фишинг – попытка выманить реквизиты вашей банковской карты, чтобы украсть с нее деньги. Всегда проверяйте адрес сайта и не вводите данные на сомнительных страницах.

Цифровая гигиена. Правила

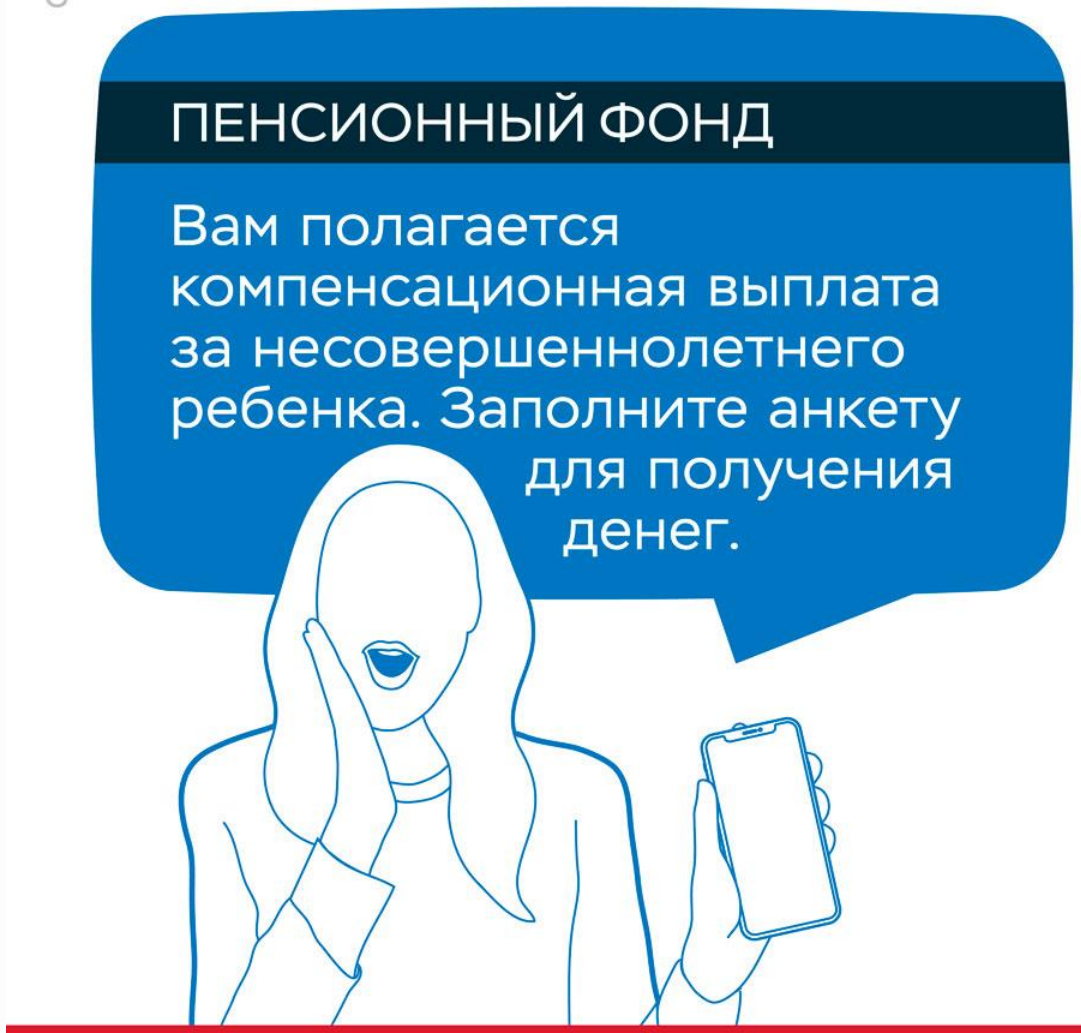


Преступники часто рассылают письма от имени популярных сервисов. Адрес отправителя может отличаться от настоящего всего парой символов. Ссылки в этих сообщениях ведут на фишинговые сайты или содержат вирусы, крадущие платежные данные с устройств. Не переходите по ним – сразу удаляйте подозрительные письма.

Цифровая гигиена. Правила

Вирусные и фишинговые рассылки обычно касаются самых популярных тем. Даже если вы сдавали анализ и ждете результат, не спешите следовать инструкциям незнакомого отправителя. Сначала проверьте адрес лаборатории на ее официальном сайте.

Цифровая гигиена. Правила

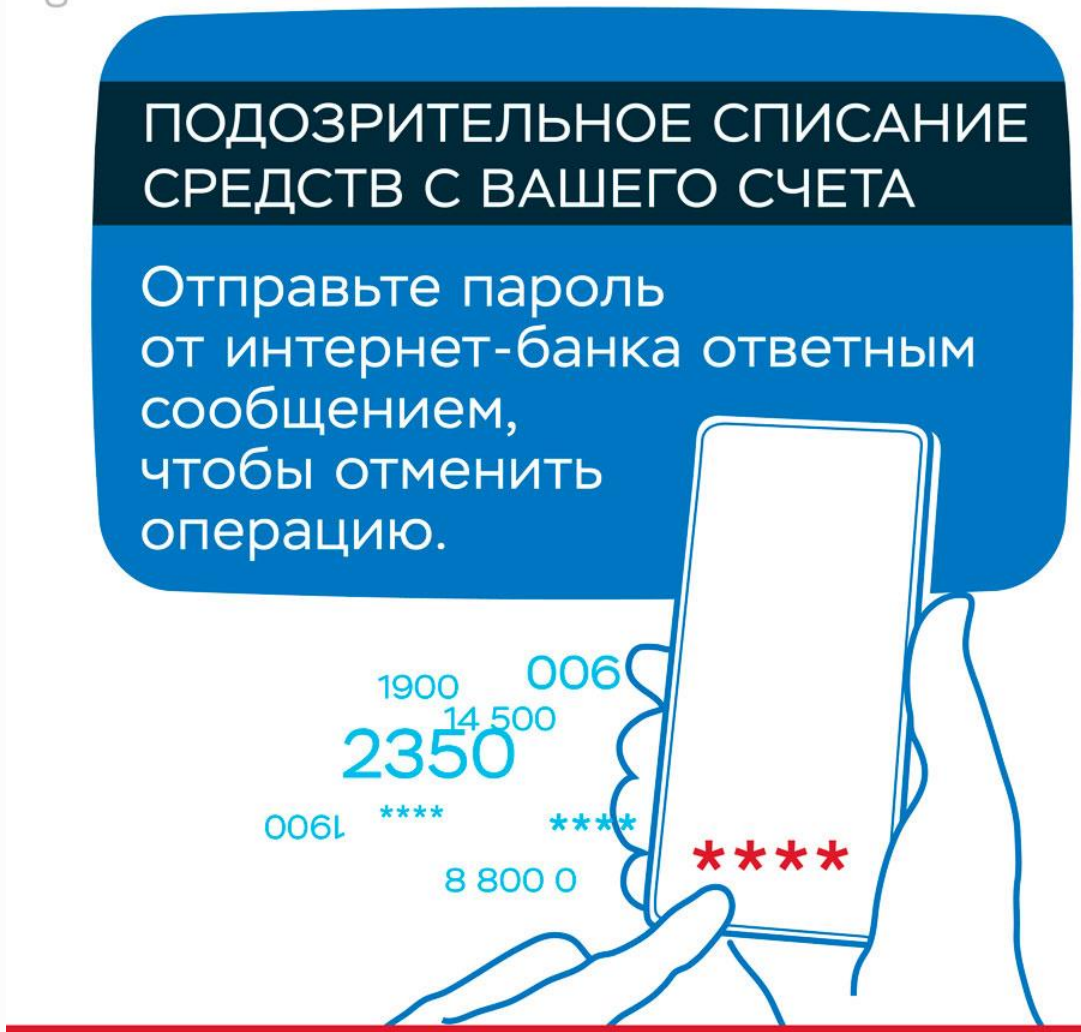


«Письма счастья» о государственных выплатах могут оказаться уловкой мошенников. Не вводите данные банковской карты на сомнительных страницах. Всегда перепроверяйте информацию о субсидиях и компенсациях в деловых СМИ или на сайтах ведомств. А еще лучше – найдите и сами прочитайте законы, указы или постановления.

Цифровая гигиена. Правила

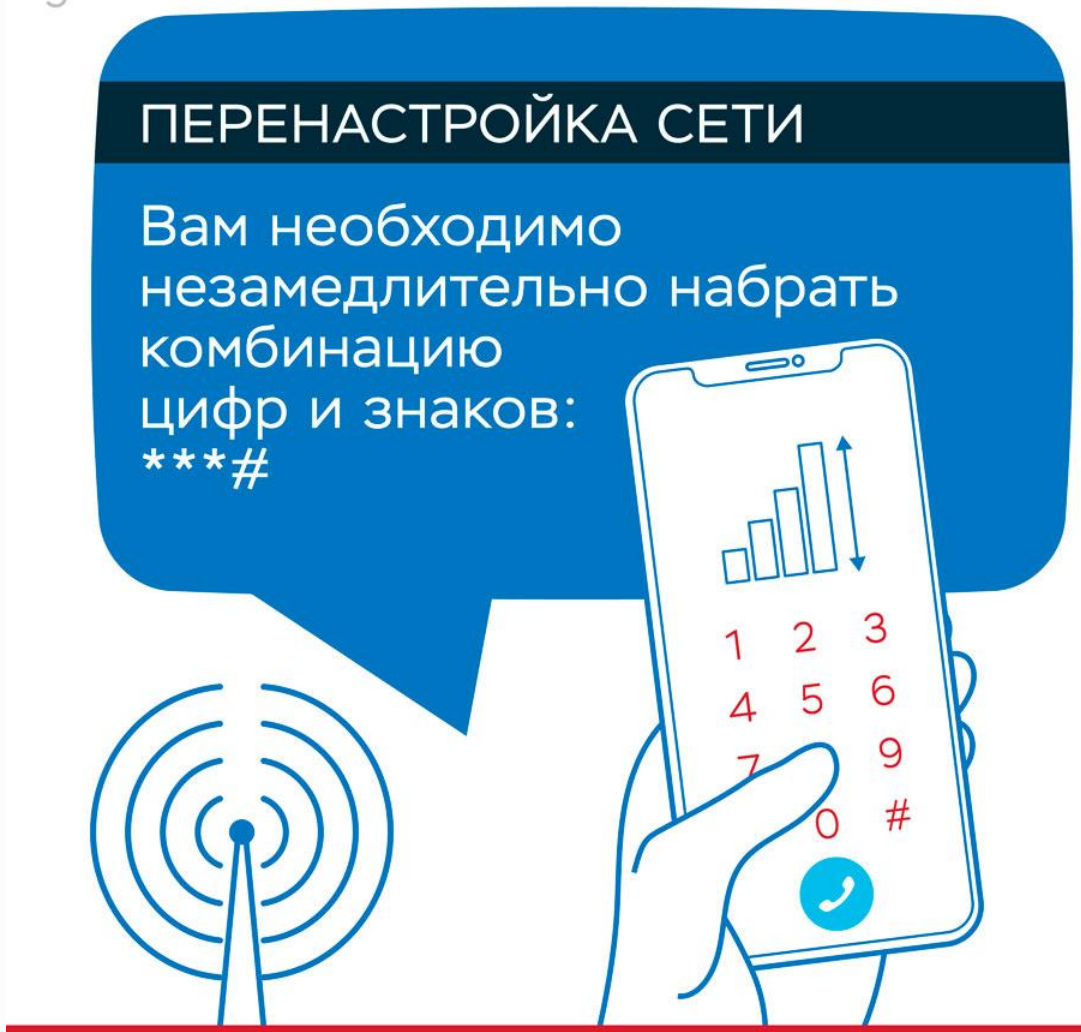
Не переходите по ссылке – сначала позвоните в банк по официальному номеру и уточните, настоящая ли это рассылка. Аферисты рассчитывают, что вы не станете проверять информацию и выполните их инструкции. А в итоге – скачаете вирус или введете свои секретные банковские данные на поддельной странице.

Цифровая гигиена. Правила



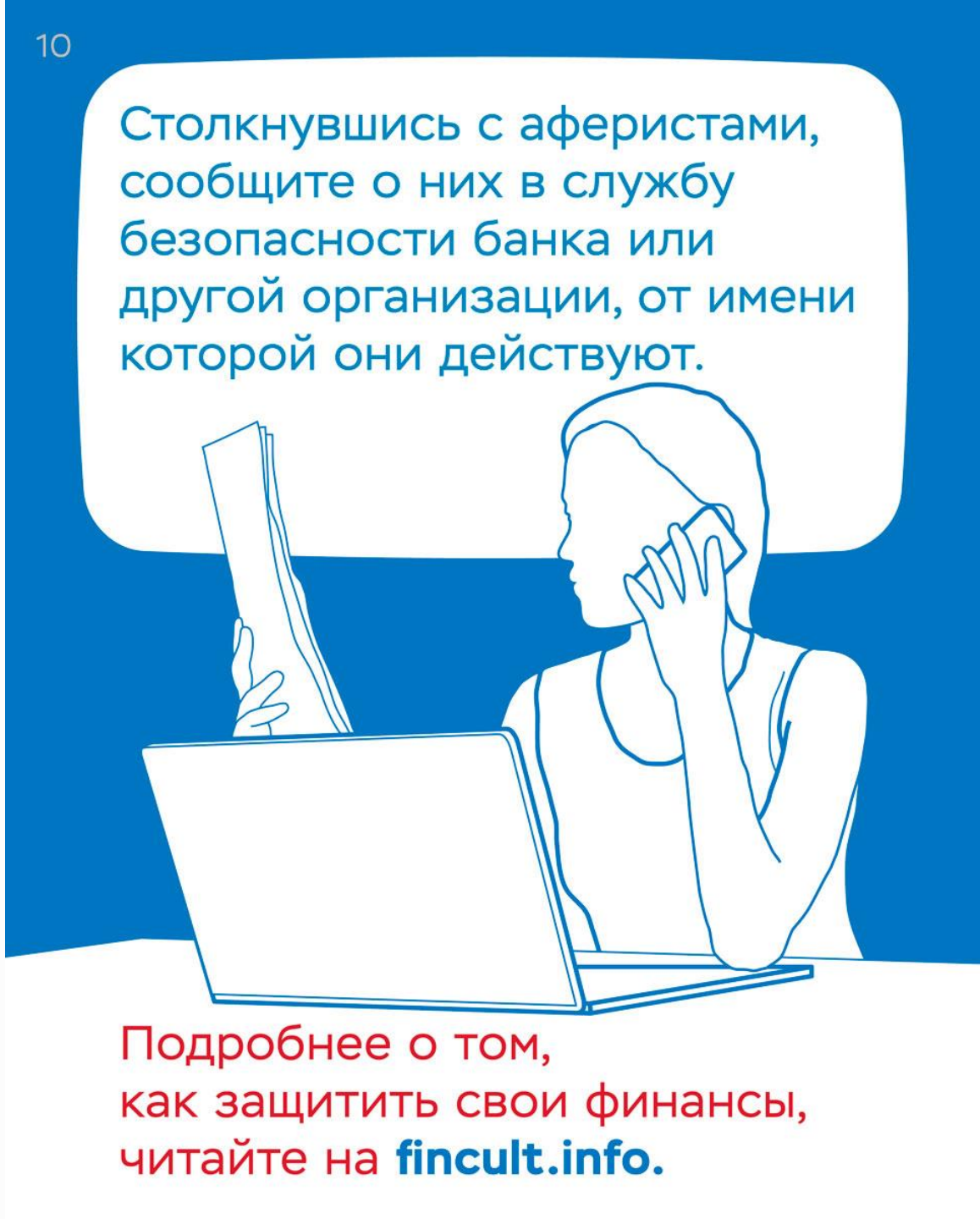
Только мошенники запрашивают пароли «для отмены операции». Никому и никогда не сообщайте данные для входа в свой онлайн-банк и коды из банковских уведомлений. Также нужно держать в секрете полные реквизиты карты, включая срок действия и три цифры с оборота. В любой непонятной ситуации сами звоните в банк по официальному номеру.

Цифровая гигиена. Правила

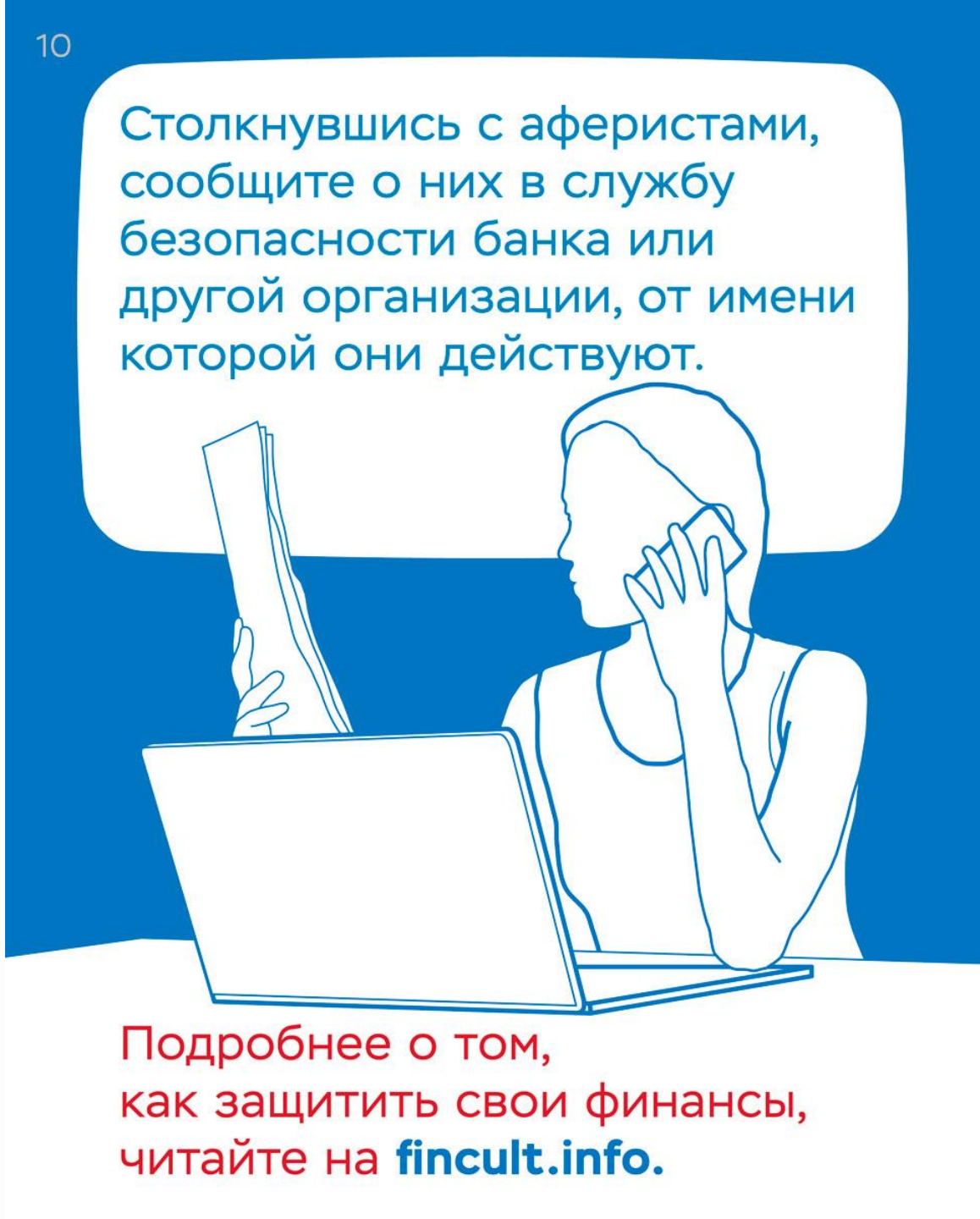


Очередная преступная схема. Любые настройки сети проходят без участия абонентов. Код, который требуют ввести на телефоне, может оказаться ключом к данным на вашем устройстве. Игнорируйте такое сообщение и передайте информацию о рассылке мошенников вашему провайдеру.

Цифровая гигиена. Правила



Цифровая гигиена. Правила



Цифровая гигиена. Кейсы

Кейс №1

В социальной сети «ВКонтакте» вам приходит личное сообщение от незнакомого вам человека следующего характера: «Привет, я в _____ году в ___ школе учился вместе с твоим отцом. Не виделись с ним тысячу лет. Пришли мне его номер, хочу с ним связаться и вспомнить молодые годы»

Цифровая гигиена. Кейсы

Кейс №2

В известной социальной сети Facebook ваш одноклассник пишет вам личное сообщение следующего характера «Привет, А***! Мне прислали твое фото. Посмотри https://foto-j9. net/a»

Цифровая гигиена. Кейсы

Кейс №3

В социальной сети ВКонтакте к вам на страничку зашел человек, на аватарке которого изображена ваша фотография, а в профиле указаны все ваши личные данные».

Цифровая гигиена. Кейсы

Кейс №4

В известной социальной сети «ВКонтакте» вам приходит сообщение от друга с текстом: «Привет! У меня проблемы, пришли срочно 1000 на эту карту сбера потом объясню!»

Цифровая гигиена. Кейсы

Кейс №5

В социальной сети «ВКонтакте» вам приходит сообщение от друга сделать репост публикации, в которой содержится не совсем для вас понятная информация о важности людям славянского происхождения объединяться, подкрепленная историческими сводками, фотографиями с непонятной символикой.

Цифровая гигиена. Кейсы

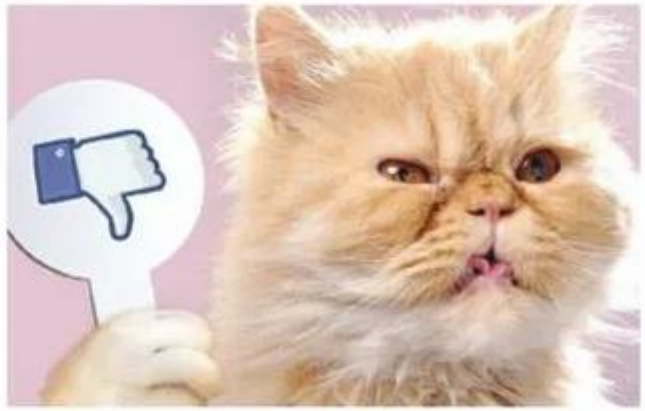
Кейс №6

В нескольких чатах в мессенджере WhatsApp вы увидели сообщение, массово распространяемое участниками беседы, со следующим содержанием: «У меня дядя работает в полиции. Он сказал, что сейчас под предлогом чем-то помочь в тачке детей заталкивают и увозят,а ещё щас раздают бесплатные живачки, а это оказывается спайс, в загородном уже увезли на скорой пару детей, ели откачали. Предупредите детей, пусть будут осторожнее».

Цифровая гигиена. Кейсы

Кейс №7

В социальной сети «ВКонтакте» в одной из групп, на которую вы подписаны, появился следующий пост, в котором сказано о закрытии приюта для животных. К посту прикреплены несколько фотографий собак. В сообщении сказано, что большинство животных уже успели раздать, однако, если не заберут оставшихся щенят, их усыпят. Прикреплен номер телефона по которому можно позвонить и забрать питомца



У ВАС ВСЕ ПОЛУЧИТСЯ!
ЭТО ТОЧНО!
МЫ УВЕРЕНЫ В ЭТОМ!

Спасибо за внимание!