SCS SBER CYBER SECURITY

Как тебя обманывают в цифровом мире

или что такое **киберграмотность**

Что происходит в кибермире?

Фейки

Телефонное мошенничество

Взломы устройств

Утечки персональных данных

Фишинг

Вредоносное ПО

Злоумышленники в соцсетях

Угон аккаунтов

Что нужно мошенникам?

КРАЖА ЛИЧНОСТИ ДЕНЕГ

>1 мин.

необходимо чтобы получить данные паспорта и личную почту по фото посадочного талона

в 70%

случаев люди сами переводят деньги или предоставляют свои платежные данные

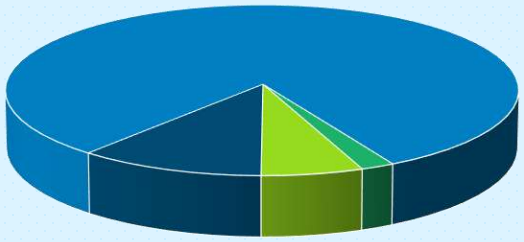
Засада в твоём любимом мире

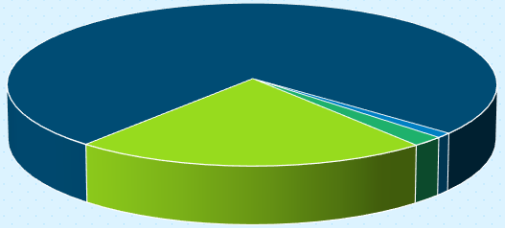
Что может сделать мошенник, взломав твою почту или устройство

- Рассылка писем от твоего имени
- Использование твоего списка контактов
- Взлом твоих аккаунтов в соцсетях
- Хищение твоих денег
- Шантаж с использованием твоей личной информации

Социальная инженерия — угроза №1

	2012	2017	2022
Социальная инженерия	11%	75%	91%
Фишинг	2%	2%	8%
Вирусы	6%	22%	1%
Скимминг	81%	1%	





2012 2017 2022

Социальная инженерия считается одним из самых разрушительных и опасных методов воздействия на человека

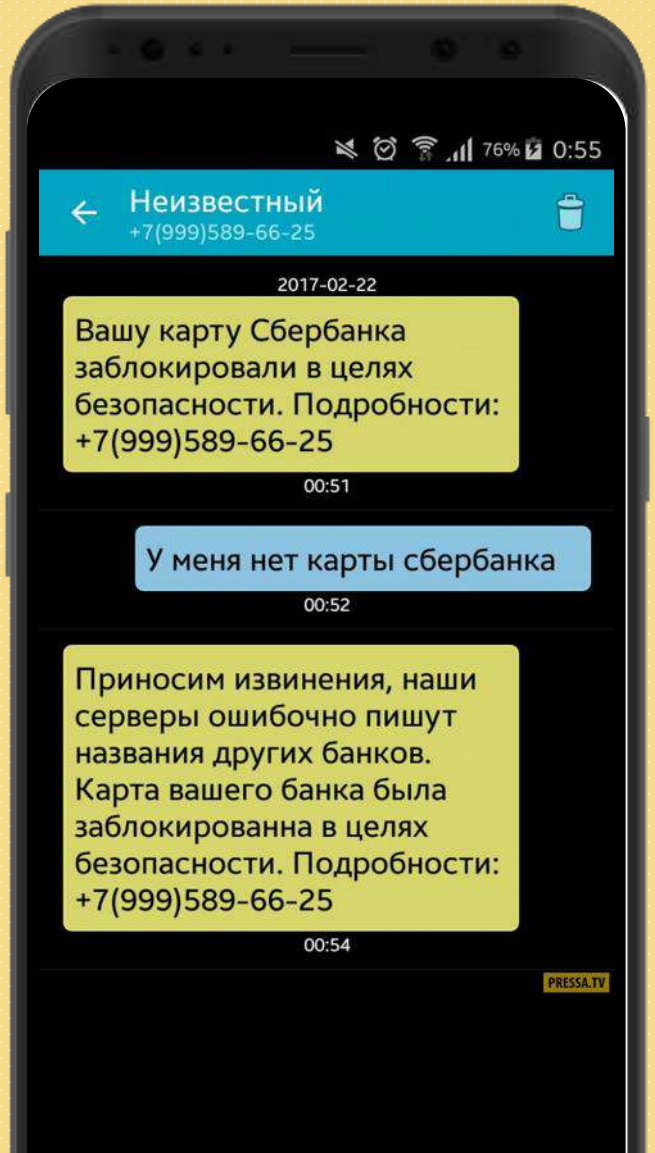
1. Телефонное мошенничество
2. SMS – мошенничество

3. Фишинговые письма
4. Мошенничество в сети Интернет
5. Мошенничество в социальных сетях

Телефонное мошенничество

АЛЛО....:с

Разнообразие тем телефонного мошенничества



Примите участие в расследовании...

Помогите поймать нечестного сотрудника...

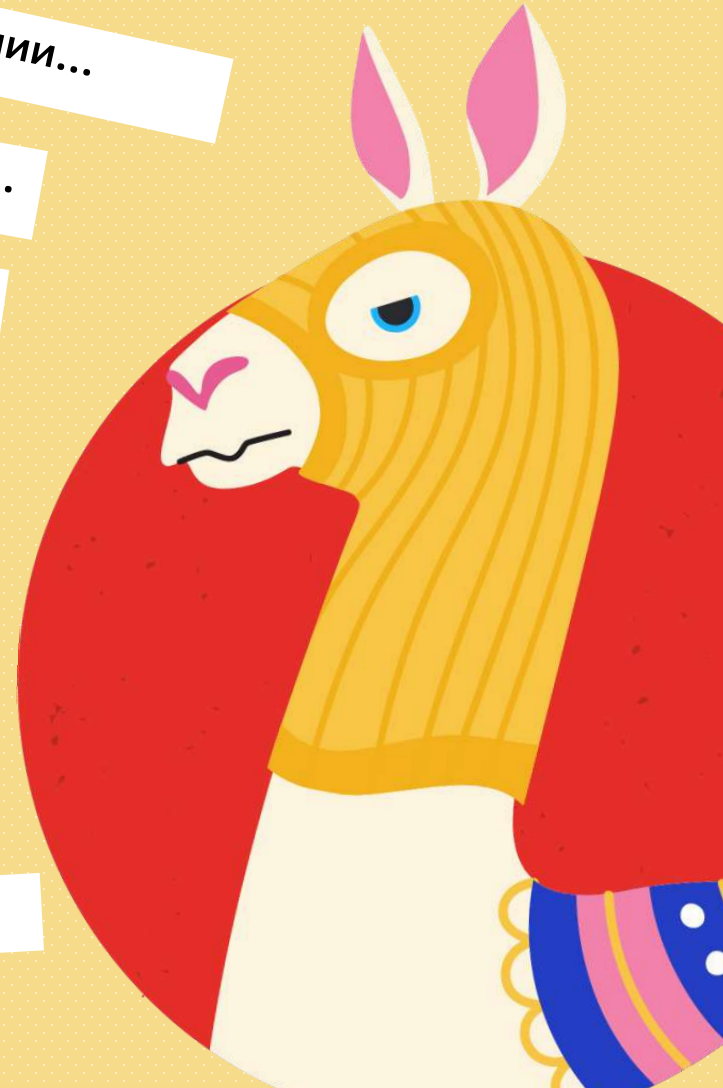
С Вашего счета хотят перевести деньги в другом городе...

На Вас оформили кредит...

Продиктуйте код для отмены мошеннической операции...

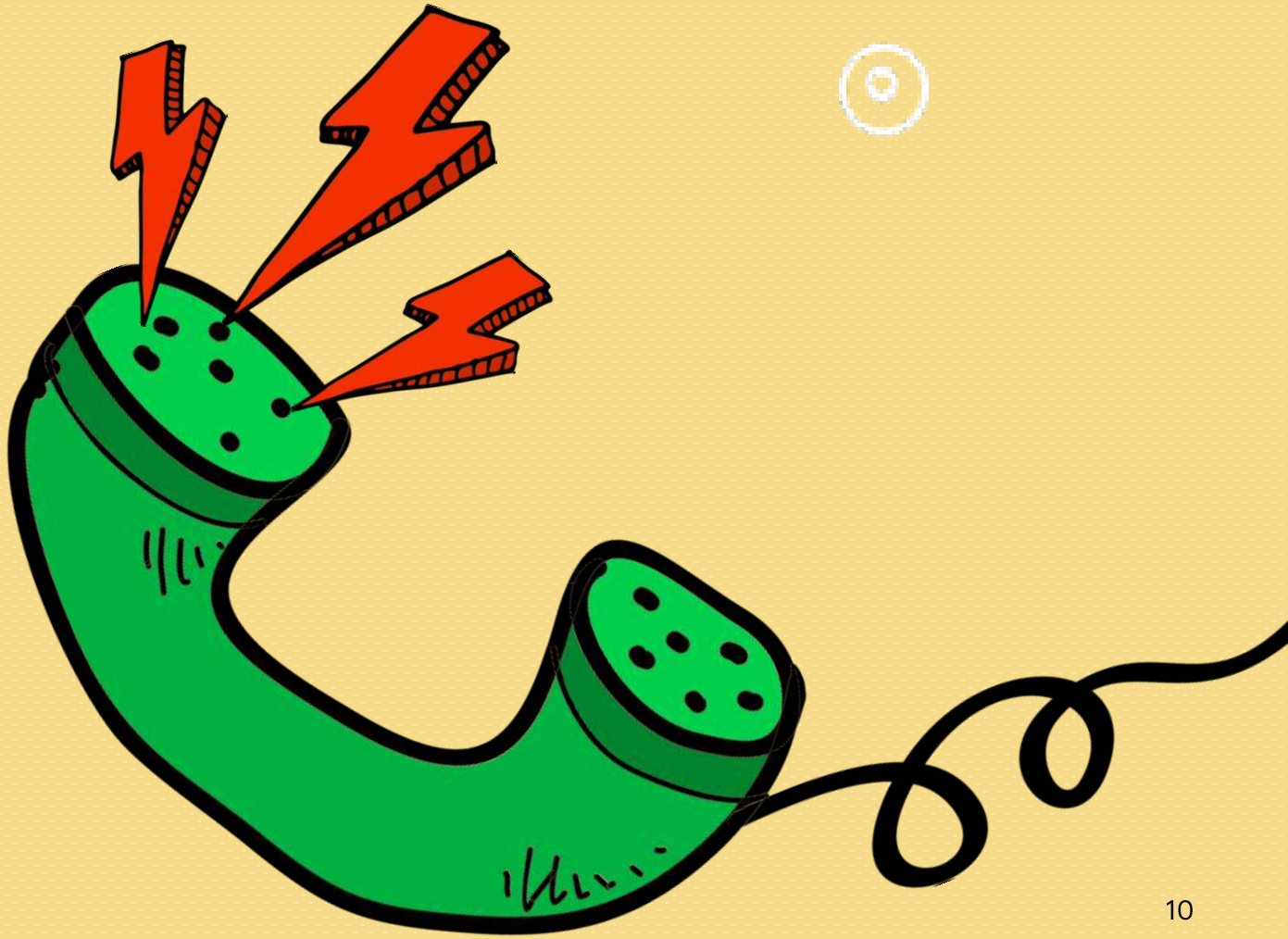
Робот: Ваша карта заблокирована, перезвоните, пожалуйста по номеру...

Голосовой помощник: сообщите смс-код



Звонок жертве мошенничества...

А ТЫ знаешь, что делать, когда позвонит мошенник?



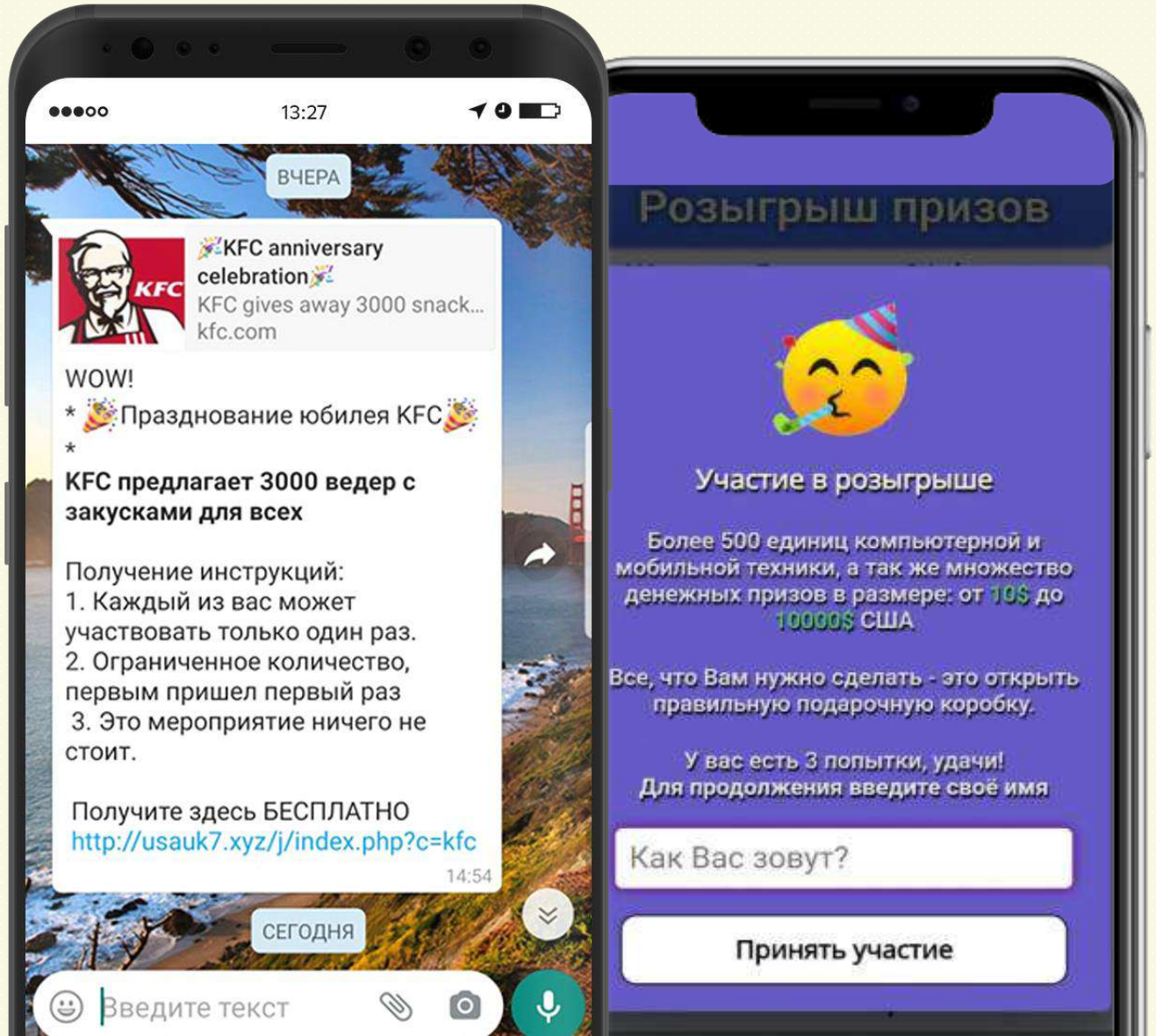
Как защитить себя

1. Не торопитесь!
   Внимательно проверяйте входящий номер
2. Если звонок будет с другого номера,
   он отобразится как неизвестный
3. Не совершайте никаких операций
   по инструкциям звонящего
4. Сразу заканчивайте разговор. Работник банка никогда не попросит у вас CVV/CVC-код, логин, пароль от СберБанк Онлайн или коды из СМС
5. Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся

Фишинговые письма

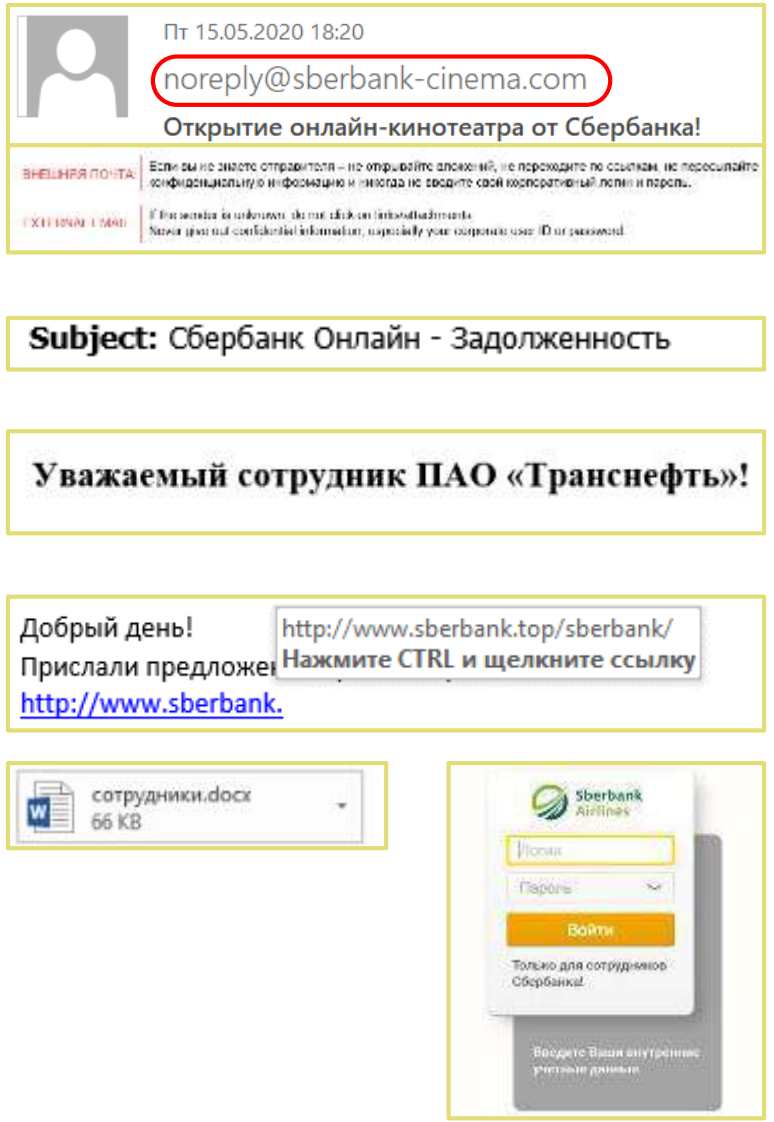
Как понять, что письмо фишинговое?

Фишинг -
вид интернет-мошенничества с использованием рассылок вредоносных электронных писем с целью получения доступа к конфиденциальным данным пользователей (логинам, паролям и т.д.)



Как защитить себя?

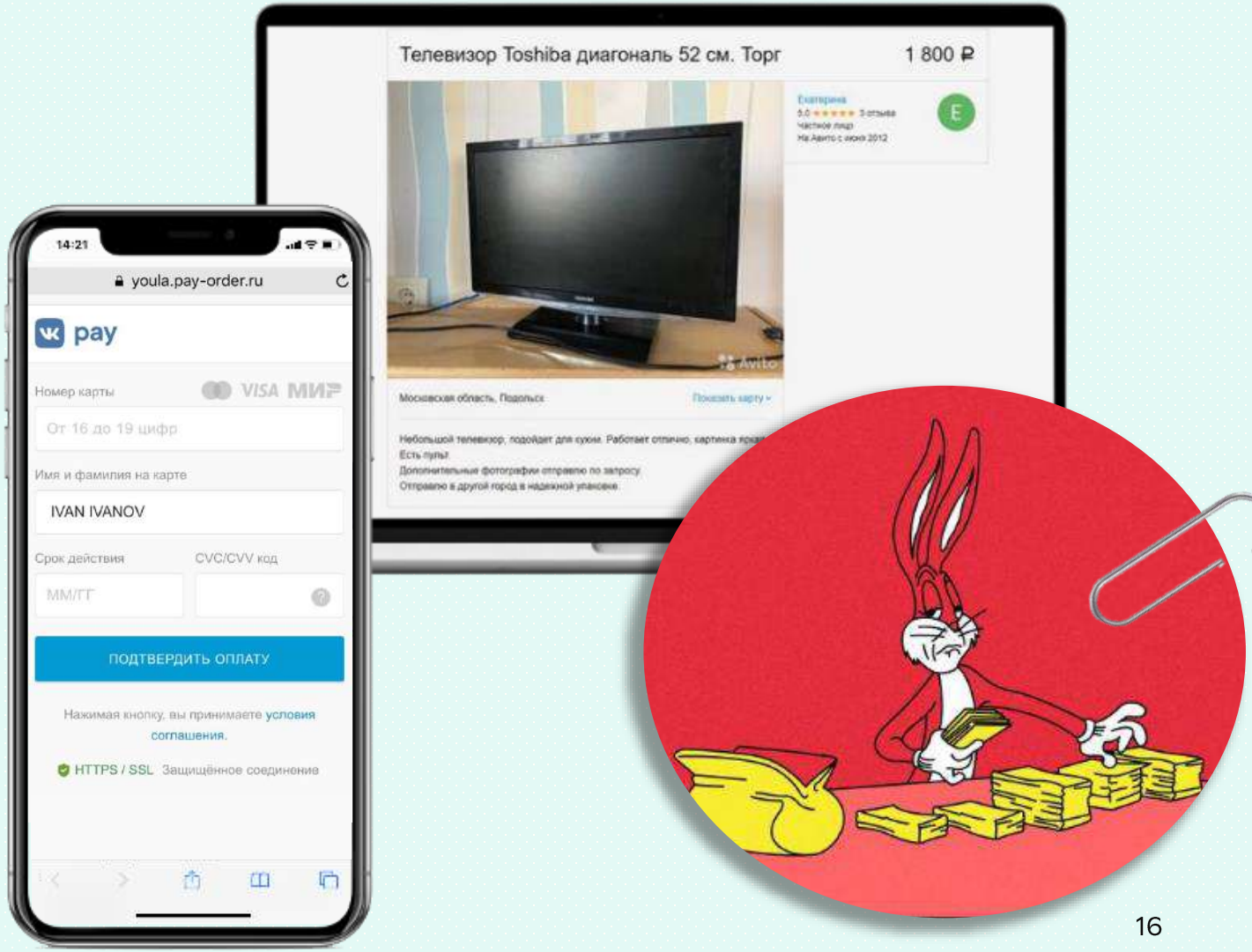
1. Обращайте внимание на домен. Мошенники обычно используют общедоступные почтовые домены gmail.com, mail.ru и т.п., или покупают домены, похожие на официальные имена компаний, чтобы ввести получателя в заблуждение.
2. Вас должно насторожить, если тема, контент письма или название файлов побуждают вас к немедленному действию.
3. Обращайте внимание на обращение и подпись. Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга. Контакты могут быть недостоверные, проверьте их на официальном сайте компании.
4. Не переходите по ссылкам, не кликайте на подозрительные объекты. Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании.
5. Будьте осторожны с вложениями, открывайте только те, которые ждали.
6. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы.
7. Не отвечайте на подозрительные письма.



Угрозы
в сети Интернет

Покупка в Интернет по выгодной цене с предоплатой

1. Мошенники размещают фиктивное объявление о продаже товара по очень выгодной цене
2. Клиент связывается с мошенником, который сообщает, что на данный товар несколько покупателей, и для того, чтобы забронировать товар, клиент должен внести предоплату
3. Покупатель осуществляет перевод в пользу неизвестных
4. После внесения предоплаты продавец перестает отвечать на звонки и сообщения от покупателя



Угрозы в киберпространстве

Киберггруминг

выманивание интимных фото ребенка с целью последующего шантажа

Хеппислепинг

видеоролики с записями реальных сцен насилия

Буллицид

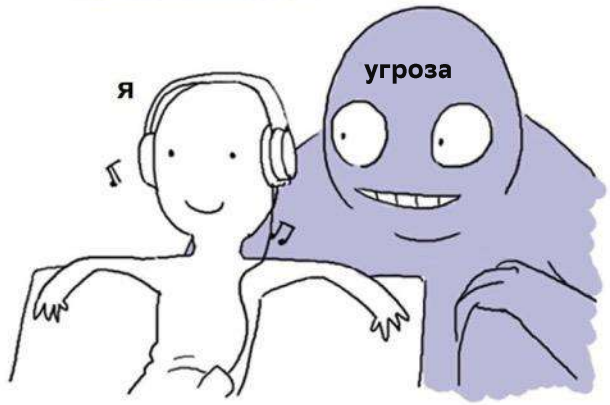
доведение ребенка до самоубийства путем психоло-гического насилия

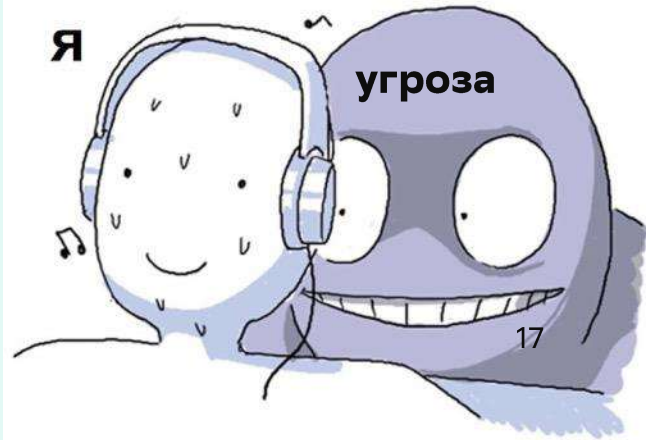
Кибербуллинг троллинг, моббинг

оскорбления, угрозы, травля детей в кибер-пространстве

Лудомания игромания, гэмблинг

виды цифровой зависимости ребенка



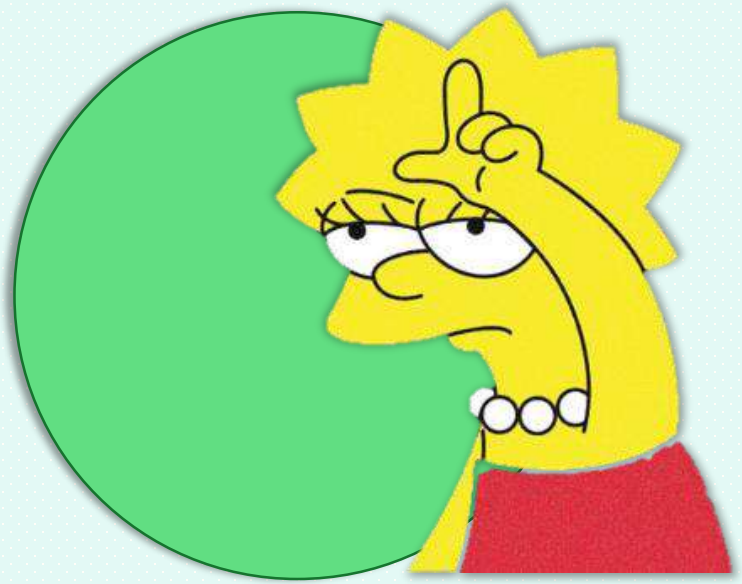


Манипуляторы

Ждут тебя в сектах и «группах смерти»

Зовут тебя на баррикады

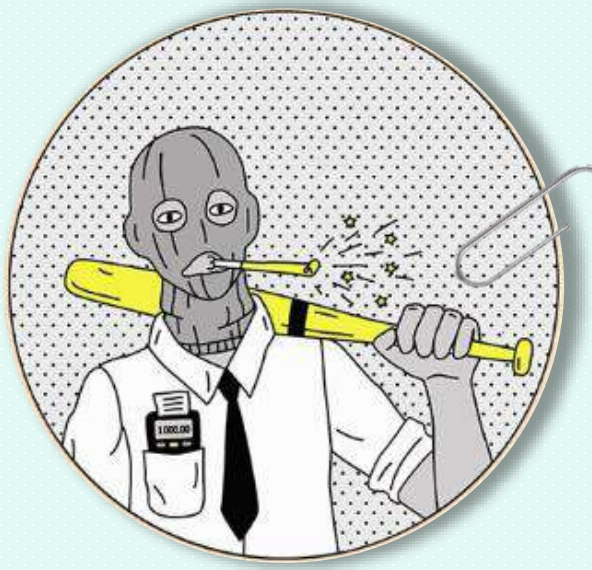
Заставляют тебя делать то,
что тебе не нужно



Думай, а свои ли желания ты выполняешь!

Маньяки

За авой Кати из 10Б,
может скрываться 40 летний мужик
с комплексами и нездоровым интересом



Смешно?

2021 год побил рекорд по количеству
обращений на горячие линии за 4 года

Мошенники

Драгдилеры

Хейтеры

Хакеры

Маньяки и психически нездоровые люди

Манипуляторы

Думаешь, что тебя это не касается?

Что знает о тебе интернет:

Интернет-магазины

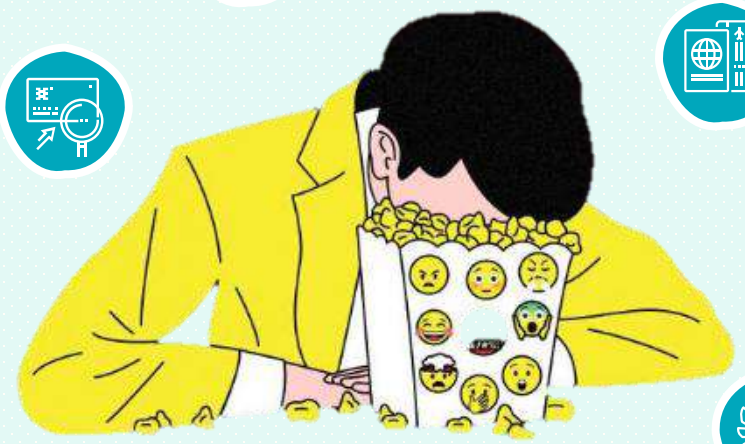
- Предпочтения
- Платежная информация
- Физические параметры (размеры обуви и одежды)

Социальные сети

- Друзья и знакомые
- Политические и религиозные активности
- Хобби

Поисковые системы

- История запросов
- Действия на сайте
- Выбор товаров и услуг
- Идентификаторы устройств
- Данные об учетных записях



Билеты

- Данные о перелётах, поездках и попутчиках

Государственные услуги

- Паспорт и другие документы
- Состав семьи
- Состояние здоровья

Службы доставки

- Место жительства и работы
- Уровень дохода

Такси и каршеринг

- Время и маршруты поездок

Карты и навигаторы

- Местоположение и передвижения
- Любимые места
- Модели поведения

Любое наше действие в сети оставляет цифровой след

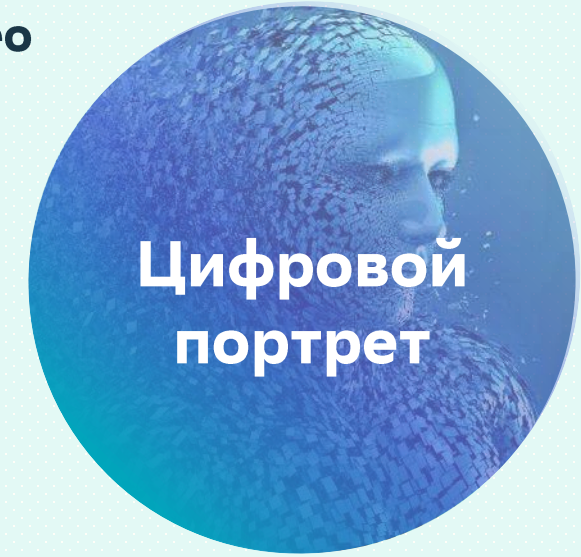
регистрация на сайтах

фото и видео

лайки в соцсетях

посты и репосты

комментарии к постам



КНОПКИ В ИНТЕРНЕТЕ **НЕТ**

ИНФОРМАЦИЯ, ПОПАВШАЯ В СЕТЬ, ОСТАЕТСЯ ТАМ **НАВСЕГДА**

Мошенничество в социальных сетях

Как «утекают» ваши персональные данные

При размещении данных на сайте вы фактически теряете контроль за их использованием и распространением

В пользовательских соглашениях есть пункты, которые гласят:

«В случае перехода прав собственности или контроля над всеми или частью наших Продуктов или их активов к другому лицу мы можем передать вашу информацию новому владельцу.»

«Администрация Сайта считает, что Пользователь осознает, что информация на Сайте, размещаемая Пользователем о себе, может становиться доступной для других Пользователей Сайта и пользователей Интернета, может быть скопирована и распространена такими пользователями.»

«Мы делимся вашими данными с нашими сторонними поставщиками услуг, которых мы используем, чтобы предоставлять вам доступ к Платформе. Мы также предоставляем вашу информацию нашим деловым партнерам, рекламодателям, операторам аналитических и поисковых систем.»

«Публично размещая контент посредством Твитов, вы, тем самым, указываете нам раскрывать эту информацию в объеме настолько широком, насколько это возможно.»

Осторожно, скаммеры!

1. Под видом романтических отношений: знакомства через Интернет, социальные сети, службы подбора «невест по переписке», предлагают потратить средства на любимого человека:
2. Оплатить:
   - пересылку подарка,
   - налоги на таможне для доставки подарка,
   - переезд,
   - деньги в долг
3. После получения средств злоумышленники перестают отвечать на звонки и сообщения.

Чаще всего жених и невеста проживают в разных странах.

Все схемы имеют одну цель — побудить человека к отправке денежных средств.

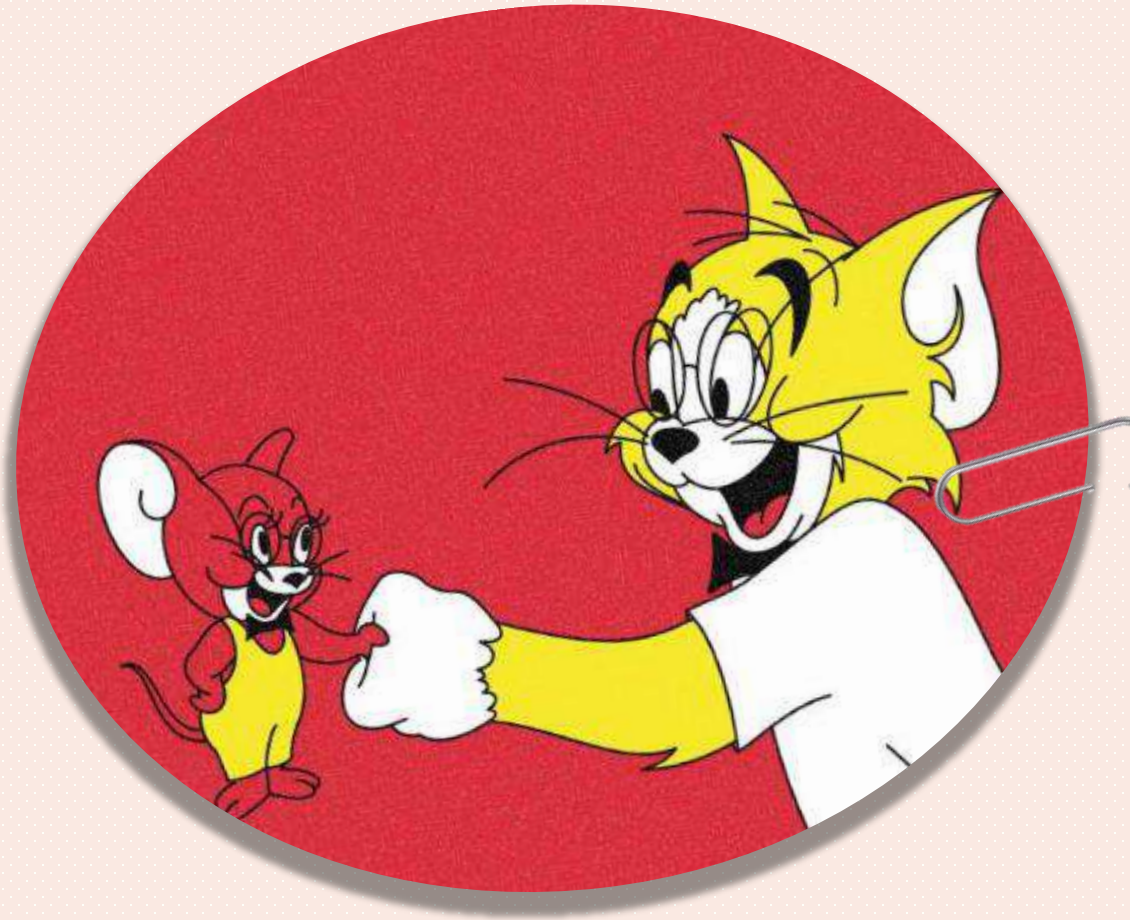
Осторожно, хейтеры!

1. В соцсети создается подставной профиль, например, симпатичной девушки
2. С этого аккаунта пишутся оскорбления / провокации другим пользователям
3. Жертвы буллинга начинают интересоваться тем, кто шлет им гадости и переходят на страницу «обидчицы»
4. Не найдя никакой полезной информации, кликают по единственной размещенной на странице ссылке, которая ведет на фишинговый сайт
5. Фишинговый сайт копирует страницу входа на другую популярную соцсеть

Если введете свой логин и пароль, мошенник получит контроль над вашим аккаунтом

Схема: Бизнес-партнёр

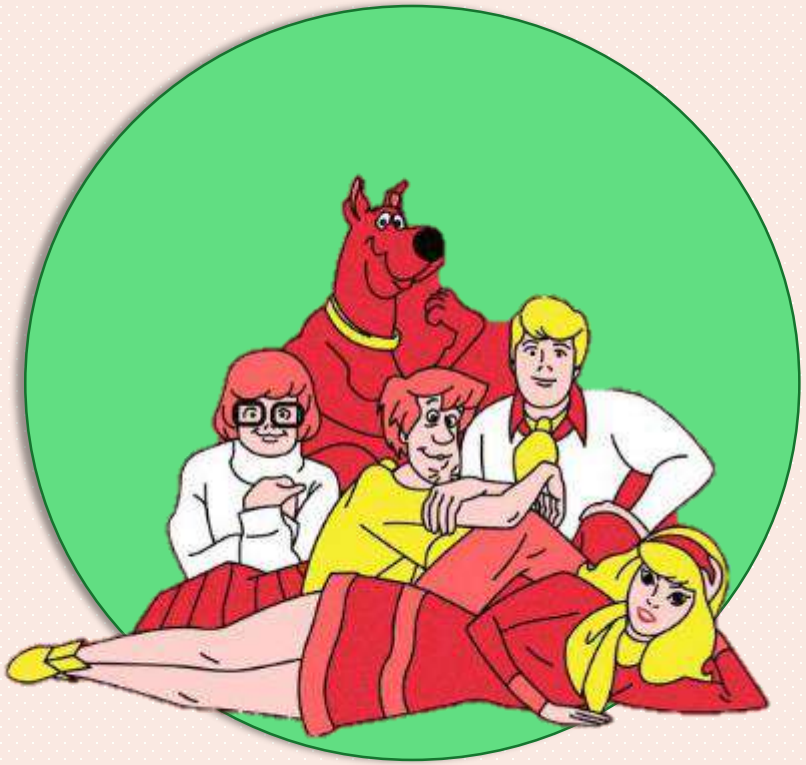
1. Фейковая страница успешного бизнесмена, который во всех красках показывает свою роскошную жизнь
2. Всем, кто хочет также, «предприниматель» предлагает вложиться в его новый проект с гарантией высокого дохода, когда средств инвесторов наберется достаточно, чтобы «начать работу»
3. Особые условия для участия действуют «только 24 часа», а количество мест «строго ограничено»



После «вложения денег» в несуществующий проект инвестор попадает в черный список, а сам мошеннический аккаунт исчезает

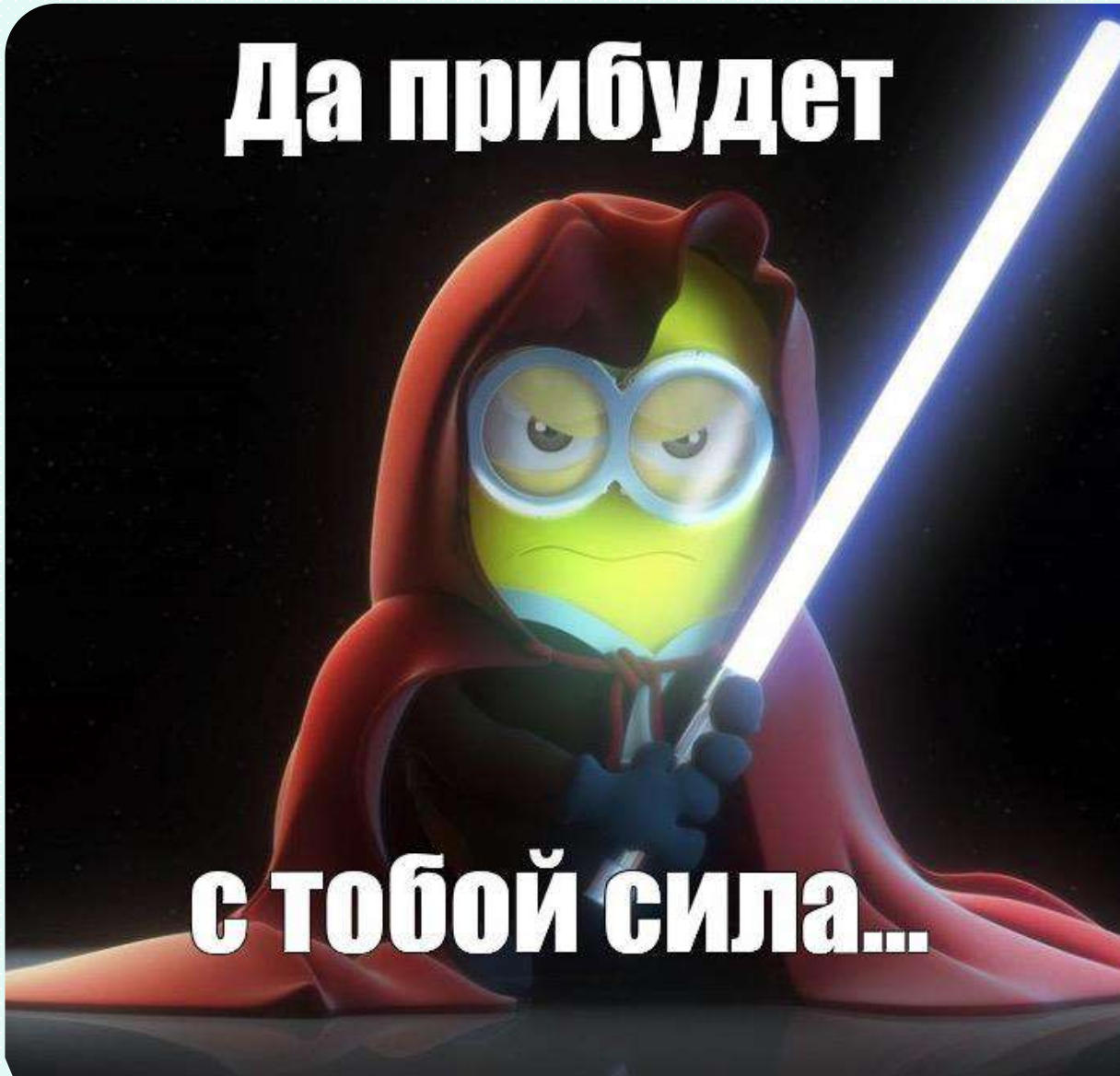
Как защитить себя?

1. Установите на свои аккаунты сложные пароли
2. Проверьте настройки устройства и приложений – что, как и куда сохраняется, передается, с чем синхронизировано. При необходимости меняем настройки
3. Не указывайте в профиле личные, не общедоступные контактные данные (номер телефона, адрес личной электронной почты)
4. Не отправляйте в личных сообщениях видео и фотографии пользователям, которых ты не знаешь в реальной жизни
5. Отправляя кому-либо личную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает
6. В случае сомнений в личности вашего нового знакомого предложите визуальный контакт и понаблюдайте за реакцией
7. Будьте бдительны

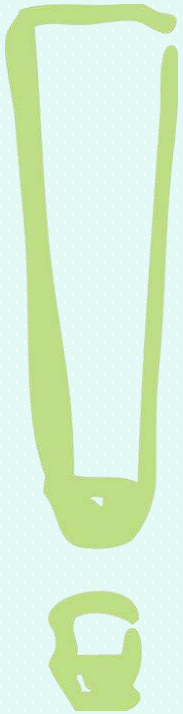


Как защитить себя в киберпространстве

- Защищай свои устройства
- Используй сложные пароли
- Настрой безопасность данных
- Соблюдай правила общения
- Будь финансово грамотным



Знай, как выглядит вирусная угроза



Произвольно запускаются программы, удаляются файлы и папки, искажается их содержимое

Ваши друзья получают от вас сообщения, которые вы не отправляли, наблюдаются частые зависания и сбои системы

На экране появляются подозрительные сообщения, рекламные окна

Основные источники вирусного заражения

НА КОМПЬЮТЕРАХ

- Переход по ссылкам и открытие вложенных файлов в письмах от неизвестных отправителей
- Скачивание и установка нелицензионного ПО
- Подключение неизвестных съемных носителей

НА МОБИЛЬНЫХ УСТРОЙСТВАХ

- Скачивание и установка приложений из неавторизованных источников
- Отсутствие Антивируса
- Использование открытых Wi-Fi сетей
- Переход по ссылкам из сообщений в соцсетях и мессенджерах

Сократи цифровой след

- Сначала думай, потом публикуй
- Настрой конфиденциальность на сайтах, которые часто посещаешь, особенно в соц. сетях
- Удали или скорректируй старые данные
- Регулярно чисти **cookie**

Береги личное пространство

Обнови настройки приватности

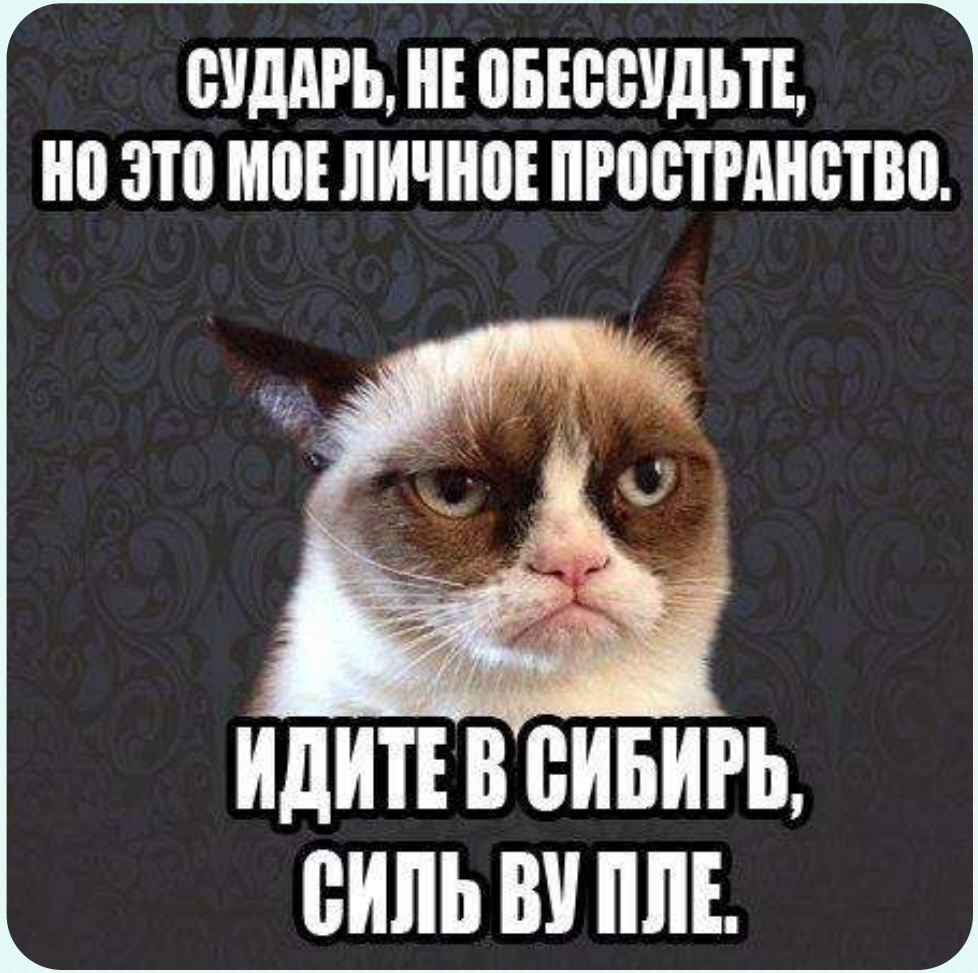
НЕ делись большим объемом информации

НЕ выкладывай фото документов

НЕ размещай информацию о родственниках

НЕ добавляй незнакомцев в друзья

НЕ используй метки и хештеги геолокации



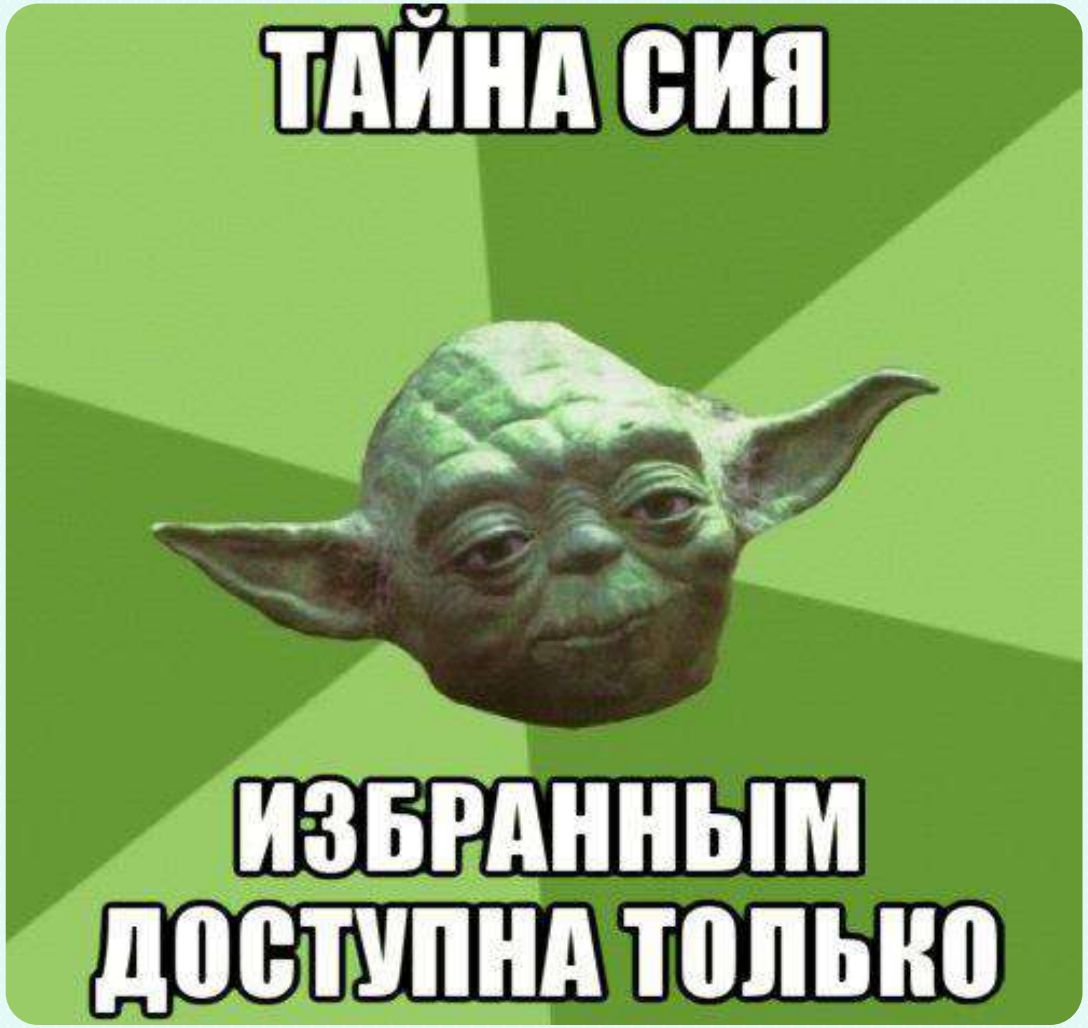
Настрой конфиденциальность в соцсетях

Публикуемые записи «по умолчанию» доступны только друзьям

Если необходимо сделать запись открытой для всех, настройку «по умолчанию» можно отменить для одной определенной записи

Не указывай в профиле личные, не общедоступные контактные данные (номер телефона, адрес личной электронной почты)

Личные данные видят только пользователи, которые входят в круг «друзей»



Соблюдай правила общения

Не выкладывай личную информацию (например, совместные фотографии и видео) о друзьях без их разрешения

Не отправляй в личных сообщениях видео и фотографии пользователям, которых ты не знаешь в реальной жизни

Отправляя кому-либо личную информацию, убедись в том, что адресат — действительно тот, за кого себя выдает

Заведи несколько адресов электронной почты, например: частный — для личной переписки публичный — для открытой деятельности в социальных сетях и т.д.

Защищай свои устройства

- Сложные пароли
- Двухфакторная идентификация
- Официальный софт
- Осторожно с облаками
- Регулярные обновления

Используй сложные пароли

Надежный пароль должен состоять из 12 знаков (а лучше больше).
В нём необходимо использовать: **строчные и ПРОПИСНЫЕ буквы, цифры и символы**

60% пользователей используют одинаковые или похожие пароли на нескольких учетных записях

Сколько времени нужно, чтобы взломать пароль:

Кол-во знаков	Только цифры	Строчные буквы	ПРОПИСНЫЕ строчные буквы	Цифры ПРОПИСНЫЕ строчные буквы	Цифры ПРОПИСНЫЕ строчные буквы символы
8	мгновенно	5 сек.	22 мин.	1 час	8 часов
9	мгновенно	2 мин.	19 ч.	3 дня	3 недели
10	мгновенно	58 мин.	1 месяц	7 мес	5 лет
11	2 сек.	1 день	5 лет	41 год	400 лет
12	25 сек.	3 недели	300 лет	2 тыс. лет	34 тыс. лет

Пример алгоритма создания пароля:

1. Любимые фразы на русском
2. Имена любимых героев или людей
3. Названия любимых произведений, игр, КОТОРЫЕ НИКОГДА НЕ ЗАБУДЕТЕ и переведите их на латиницу:

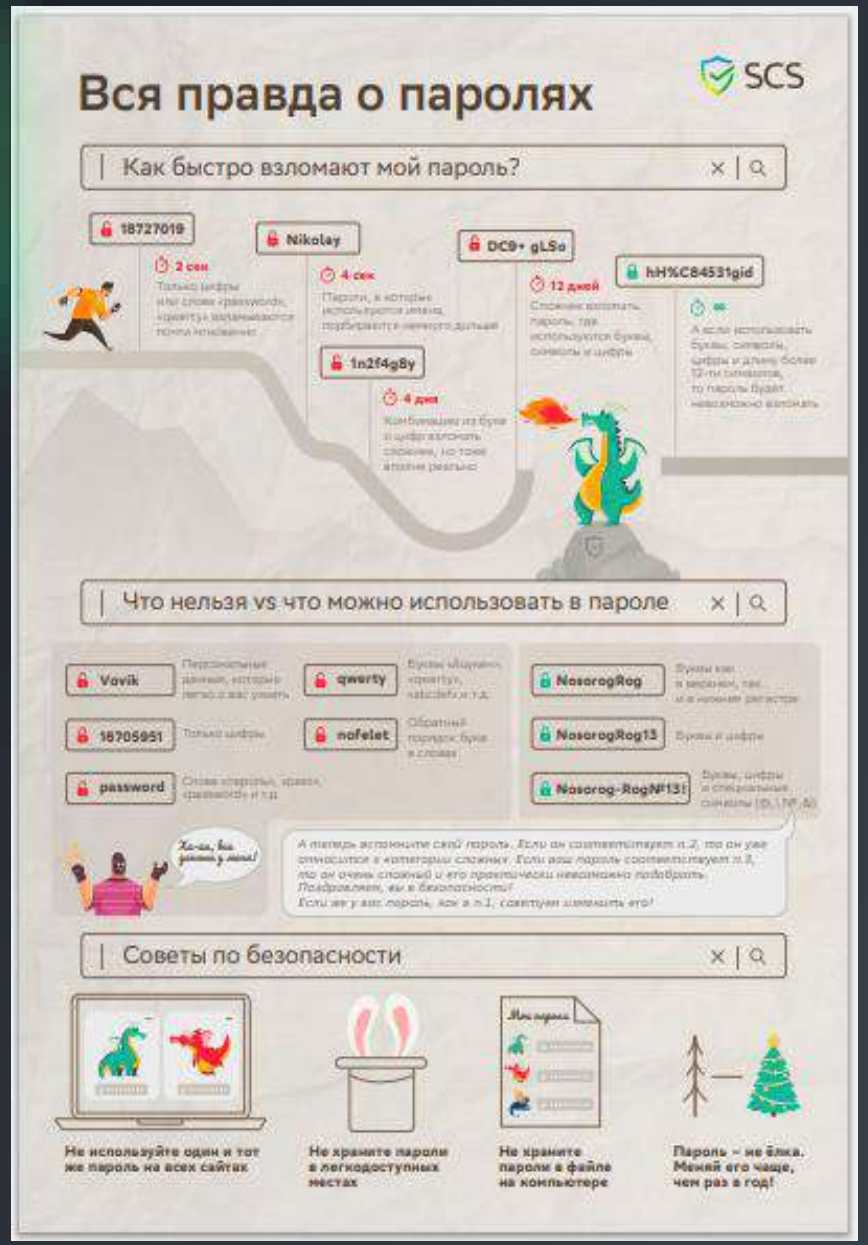
Этонаоценку? **“njyf0wtyre&**

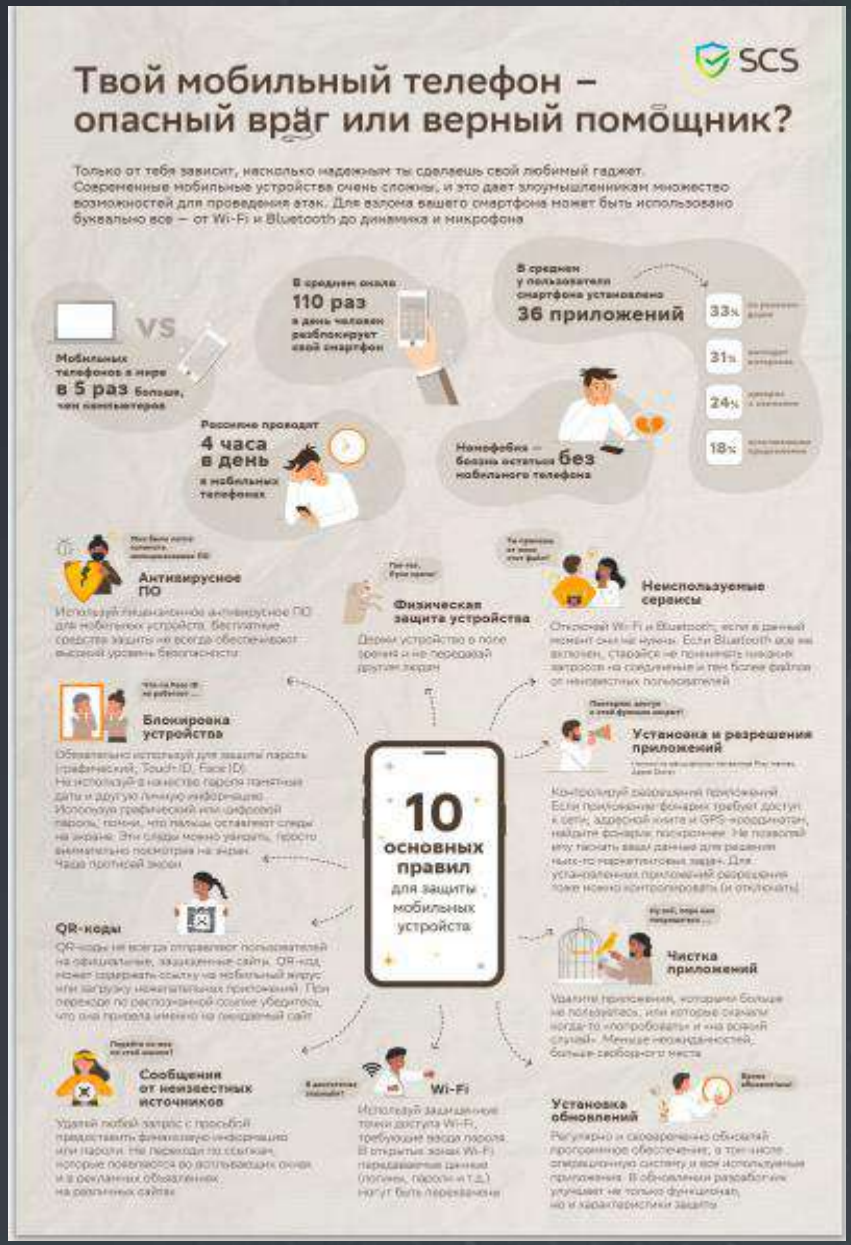
Домашнее задание будет **L0vfiytt pflfybt ,eltn**

Всёпопорядку! **Dc`g0g0hzlre!**

Скачай полезные памятки и поделись ими с друзьями

SCS SBER CYBER SECURITY

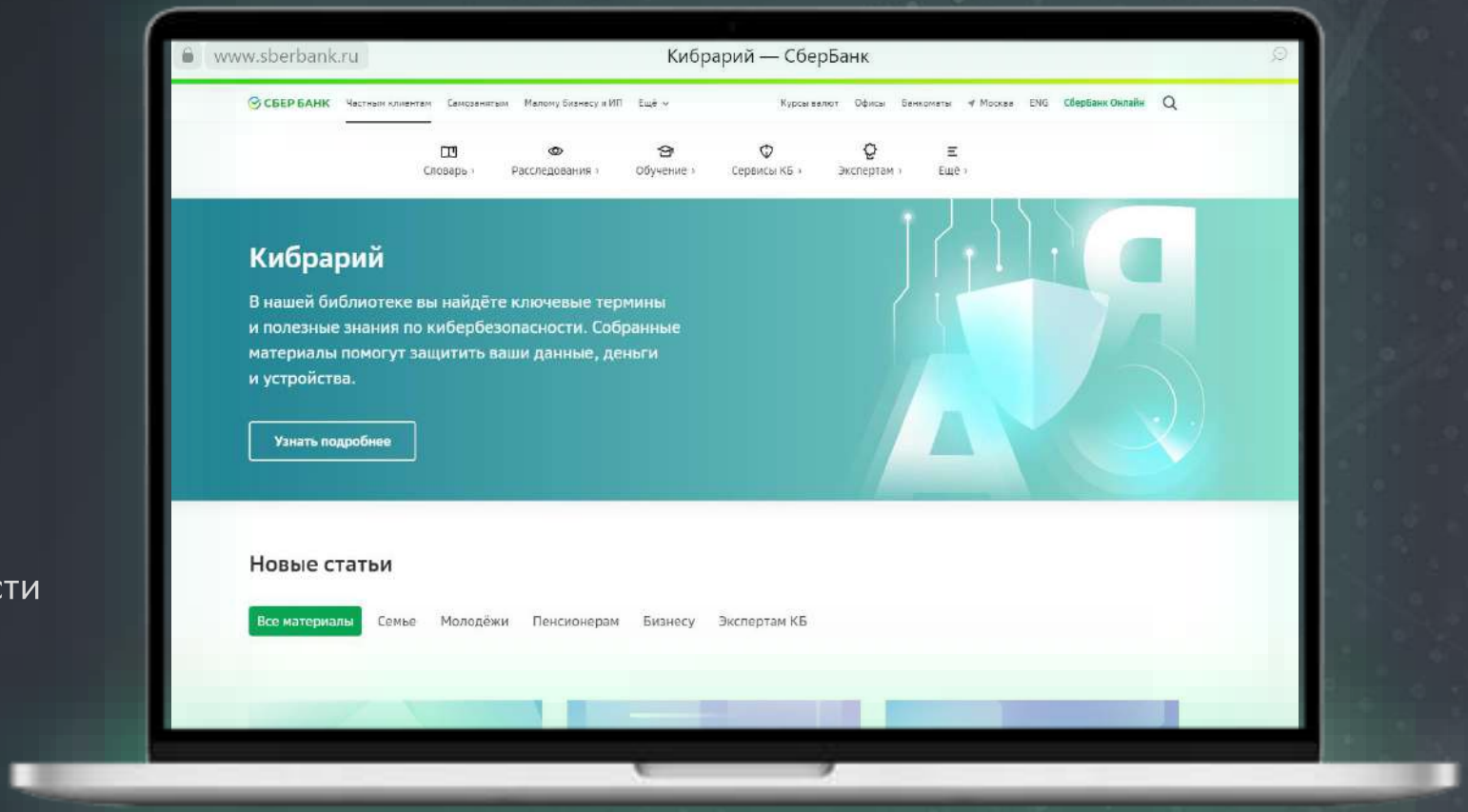




«Кибрарий» — общедоступный портал знаний для развития киберграмотности

SCS SBER CYBER SECURITY

- Советы и рекомендации для пенсионеров
- Обучающие курсы для всей семьи
- Памятки для молодежи
- Расследования
- Полезная информация от МВД
- Экспертные статьи
- Новости и Интервью по темам КБ
- Сервисы кибербезопасности Сбербанка



200+ материалов для повышения киберграмотности

100+ терминов и определений

20+ видеоматериалов по схемам мошенничества

4 курса по правилам кибербезопасности

Перейти

Будьте бдительны!

1. Запишите номера банка 900 и 8-800-555-55-50 в телефонную книгу
2. Не сообщай номер своей банковской карты, срок действия, CVV-код и код из СМС
3. Не совершайте никаких операций по инструкциям звонящего
4. Не открывайте ссылки из сообщений от незнакомых номеров
5. Установите на свои аккаунты сложные пароли
6. Устанавливайте на свои устройства программное обеспечение только из официальных источников
7. Перепроверяйте все акции на официальных сайтах и страницах в социальных сетях
8. Если для получения большой суммы денег вам сначала предлагают потратить сравнительно небольшую, будьте осторожны, это мошенничество
9. Заведите несколько адресов электронной почты для разных целей
10. Не отправляйте незнакомым людям кому-либо личную информацию
11. Проверяйте настройки устройства и приложений
12. Будьте осторожны с вложениями, открывайте только те, которые ждали
13. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы