добро.рф

Цифровая гигиена некоммерческих организаций

Шмавонян Саркис

Ведущий менеджер по работе
с образовательными организациями,
специалист по защите информации

КИБЕРПРОТЕКТ

Отсканируйте QR-код или перейдите на

play.myquiz.ru

Введите код

00670335

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

О КОМПАНИИ

> 8 ЛЕТ

на рынке решений для резервного копирования и защиты данных

> 1 500

Партнёров в России и Республике Беларусь

> 350

сотрудников

Рейтинг работодателей

2022

В рейтинге ТОП-50 лучших работодателей страны по версии Headhunter

Приоритет: Цифра 2023

2023

Лауреат премии в номинации «Информационная безопасность» за СРК Кибер Бэкап

Национальная премия Наш вклад

2023

Победитель национальной премии «Наш вклад» с образовательным проектом Кибер Забота

ПРОФ IT Инновация
Национальный конкурс ИТ-решений

2023

Победитель премии в номинации «Информационная безопасность» за СРК Кибер Бэкап

Национальный форум информационной безопасности ИНФОФОРУМ

2023

Победитель «Кубка Инфофорума» в номинации «Сделано в России»

Ассоциации и партнёры

АРПП Отечественный софт

RUS SOFT

ПКИТ

Sk Сколково

ОЭЗ Иннополис

ПРОГРАММНЫЕ ПРОДУКТЫ

СРК

Системы резервного копирования для организаций и поставщиков услуг

HCI

Гиперконвергентная система организации ИТ-инфраструктуры

DLP

Предотвращение утечек всех типов данных

EFSS/VDR

Корпоративное решение для безопасного обмена файлами

Утилита РК

Для индивидуальных пользователей

ИИ Записями Реестра российского ПО №№4160, 4161, 19458 программное обеспечение относится к сфере искусственного интеллекта

КЛЮЧЕВАЯ ПРОБЛЕМА

От потери и утечки данных никто не застрахован

> 300 млн

записей персональных данных выложено в открытый доступ в результате утечек в 2023 г.*

25%

россиян хотя бы однажды сталкивались с потерей рабочих данных

84%

россиян обеспокоены сохранностью своих данных

Россия в ТОП-5

по числу кибератак с использованием вирусов-шифровальщиков**

Среди причин:

- сбои ИТ-систем (45%)
- поломка устройства и программные ошибки (33%)
- забытый пароль или случайное удаление (25%)
- вредоносное ПО (18%)***

* Данные Роскомнадзора
** Аналитика Киберпротект
*** Исследование Киберпротект и HeadHunter

АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ

- Низкая ИТ и ИБ компетенции физических лиц и работников организаций
- Методы социальной инженерии
- Широкое применение ВПО класса шифровальщиков и RAT
- Применение в атаках и мошеннических схемах инструменты ИИ
- Отсутствуют или недостаточные средства технической защиты
- Нарушение/невыполнение требований законодательства и/или внутренних локально-нормативных актов

НОВЫЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ДАННЫХ

Особенно государство беспокоят противоправные действия с персональными данными

Ужесточение

Новое!

Обработка ПД без письменного согласия субъекта ПД либо нарушение требований к составу сведений в согласии (ч.ч.2, 2.1 ст. 13.11 КоАП РФ)

Было:

- Физ. лица: 6-10 т.р., повторное нарушение – 10-20 т.р.
- Должностные лица: 20-40 т.р., повторное нарушение – 40-100 т.р.
- ИП/Юр. лица: 30-150 т.р., повторное нарушение – 100-300 т.р. (ИП) / 300-500 т.р. (юр.лицо)

Стало (с 23.12.2023):

- Физ. лица: 10-15 т.р., повторное нарушение – 15-30 т.р.
- Должностные лица: 100-300 т.р., повторное нарушение – 100-300 т.р.
- ИП/Юр. лица: 300-700 т.р., повторное нарушение – 0,5-1 млн. (ИП) / 1-1,5 млн. (юр.лицо)

Незаконное использование принадлежащих иностранным юр. лицам и (или) иностранным гражданам информационных систем и (или) программ для ЭВМ (ст. 13.11.2 КоАП РФ)

- С 01.03.2023 г. действует запрет на передачу персональных данных и платежных документов через иностранные мессенджеры для органов власти, ГУП, МУП и финансовых организаций.
- Роскомнадзор определил список "опасных" мессенджеров: Discord, Snapchat, Skype, Microsoft Teams, Threema, Viber, WhatsApp, WeChat и Telegram.
- Штрафы для должностных лиц – 30-50 т.р., юр.лиц – 100-700 т.р.

Нарушение требований к размещению и обновлению биометрических персональных данных в ЕБС* (ст. 13.11.3 КоАП РФ)

- Штрафы для должностных лиц – 100-300 т.р., юр.лиц – 0,5-1 млн.р.

* Единая биометрическая система

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В СФЕРЕ ПД

Ст. 13.11 КоАП РФ Нарушение законодательства Российской Федерации в области персональных данных	**Штрафы**			
	Физ.лица	Дол.лица	ИП	Юр. лица
Незаконная обработка ПД или обработка ПД, несовместимая с целями сбора ПД	Первое - 2-6 т.р., повторное - 4-12 т.р.	Первое - 10-20 т.р., повторное - 20-50 т.р.	Повторное - 50-100 т.р.	Первое - 60-100 т.р., повторное - 100-300 т.р.
Обработка ПД без согласия субъекта ПД или обработка ПД с нарушением состава сведений в согласии на обработку ПД	Первое - 10-15 т.р., повторное - 15-30 т.р.	Первое - 100-300 т.р., повторное - 300-500 т.р.	Повторное - 500 т.р.-1 млн.р.	Первое - 300-700 т.р., повторное -1-1,5 млн.р.
Отсутствие публикации или неограниченного доступа к политике обработки ПД	1,5-3 т.р.	6-12 т.р.	10-20 т.р.	30-60 т.р.
Невыполнение обязанности оператора предоставлять субъекту ПД информации, касающейся обработки его ПД	2-4 т.р.	8-12 т.р.	20-30 т.р.	40-80 т.р.
Невыполнение требования субъекта ПД, его представителя или РКН об уточнении ПД, их блокировании или уничтожении в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	Первое - 2-4 т.р., повторное - 20-30 т.р.	Первое - 8-20 т.р., повторное - 30-50 т.р.	Первое - 20-40 т.р., повторное - 50-100 т.р.,	Первое - 50-90 т.р., повторное - 300-500 т.р.
Невыполнение требования о безопасном хранении ПД на материальных носителях (при обработке ПД без использования средств автоматизации)	1,5-4 т.р.	8-20 т.р.	20-40 т.р	50-100 т.р.
Невыполнение гос. и мун. органами обязанности по обезличиванию ПД либо несоблюдение требований и методов обезличивания ПД	-	6-12 т.р.	**-**	-
Невыполнение требования по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ	Первое - 30-50 т.р., повторное – 50-100 т.р.	Первое - 100-200 т.р., повторное - 500-800 т.р.	**-**	Первое - 1-6 млн.р., повторное - 6-18 млн.р.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В СФЕРЕ ПД

Статья УК РФ	Санкции
Ст. 140 УК РФ Неправомерный отказ должностного лица в предоставлении собранных документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан	Штраф в размере до 200 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет
Ст. 272 УК РФ Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	Штраф до 200 тыс. руб. или в размере ЗП или иного дохода за период до 18 мес., либо исправительные работы до 1 года, либо ограничениее свободы до 2 лет, либо принудительные работы до 2 лет, либо лишение свободы на тот же срок Если причинен крупный ущерб или совершено из корыстной заинтересованности: Штраф от 100 тыс. до 300 тыс. руб. или в размере ЗП или иного дохода за период от 1 до 2 лет, либо исправительные работы от 1 года до 2 лет, либо ограничение свободы до 4 лет, либо принудительные работы до 4 лет, либо лишение свободы на тот же срок Если совершено группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения: Штраф до 500 тыс. руб. или в размере ЗП или иного дохода за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью до 3 лет, либо ограничение свободы до 4 лет, либо принудительные работы до 5 лет, либо лишением свободы на тот же срок Если они повлекло тяжкие последствия или создали угрозу их наступления: Лишение свободы на срок до 7 лет

НОВЫЕ ЗАКОНОДАТЕЛЬНЫЕ ИНИЦИАТИВЫ

В первом чтении приняты поправки в КоАП и УК РФ, ужесточающие административную ответственность за утечки ПД и уголовную ответственность за незаконную обработку ПД

ПФЗ № 502104-8 "О внесении изменений в КоАП РФ (в части усиления ответственности за нарушение порядка обработки ПД)"

Законопроектом устанавливается:

- ответственность за неисполнение обязанности по уведомлению Роскомнадзора об утечке ПД
- увеличенные штрафы за утечки ПД
- размер штрафа за утечку зависит от вида ПД и объема утекшей информации
- повторное нарушение влечет за собой оборотные штрафы*

Ответственность будут нести:

- физ. лица
- должностные лица гос. и мун. органов и учреждений
- ИП
- юр. лица, не являющиеся гос. и мун. органами и учреждениями

ПФЗ № 502113-8 О внесении изменений в УК РФ (в части установления ответственности за незаконное использование и передачу, сбор и хранение компьютерной информации, содержащей ПД)

Законопроектом вводится новая статья 272.1, согласно которой **устанавливается уголовная ответственность** за следующие деяния:

- использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей ПД, полученной неправомерно
- создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для незаконного хранения и (или) распространения ПД

В вободы до 10 лет, принудительные работы, запрет зазависимости от деяния и вида ПД предусмотрено лишение снятия определенных должностей и ведения деятельности, а также крупные штрафы.

* Штраф рассчитывается как процент совокупного размера суммы выручки, полученной от реализации товаров, работ, услуг за календарный год, предшествующий году выявления нарушения.

ОРГАНИЗАЦИОННЫЕ МЕРЫ

Как обезопасить себя и обрабатываемые персональные данные

- Организация есть в Реестре операторов ПД Роскомнадзора

Локальные акты

- Политика обработки ПД и локальные акты по вопросам обработки ПД
- Приказ о назначении ответственного за обработку ПД
- Приказ о назначении ответственного за защиту ПД
- Приказ об утверждении перечня лиц, которым необходим допуск к ПД для выполнения должностных обязанностей

Иные меры

- На сайте опубликована политика обработки ПД
- Собирается согласие на обработку ПД в форме обратной связи на сайте
- Обеспечена безопасность помещений, в которых ведется обработка ПД
- Работников знакомят с правилами информационной безопасности при работе с ПД

ТЕХНИЧЕСКИЕ МЕРЫ

Как обезопасить себя и обрабатываемые персональные данные

Используется двухфакторная аутентификация для доступа ко всем аккаунтам (ресурсам)

Осуществляется защита каналов связи, сегментирование сети организации

Пользователи информационных систем ПД (ИСПД) используют персональные учетные записи, нет общих или обезличенных учетных записей

Ведется контроль установки ПО на серверы и ПК ИСПД

Учетные записи уволенных работников своевременно блокируются, отпускников тоже блокируется на период отпусков (если нет необходимости работать **;-)**

Проводится поиск и устранение уязвимостей

Используется антивирусная защита, базы регулярно обновляются

Проводится резервное копирование ИСПД

Проводится регулярное обновление ОС и ПО

Применяются решения, защищающие от утечек информации, класса DLP

ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

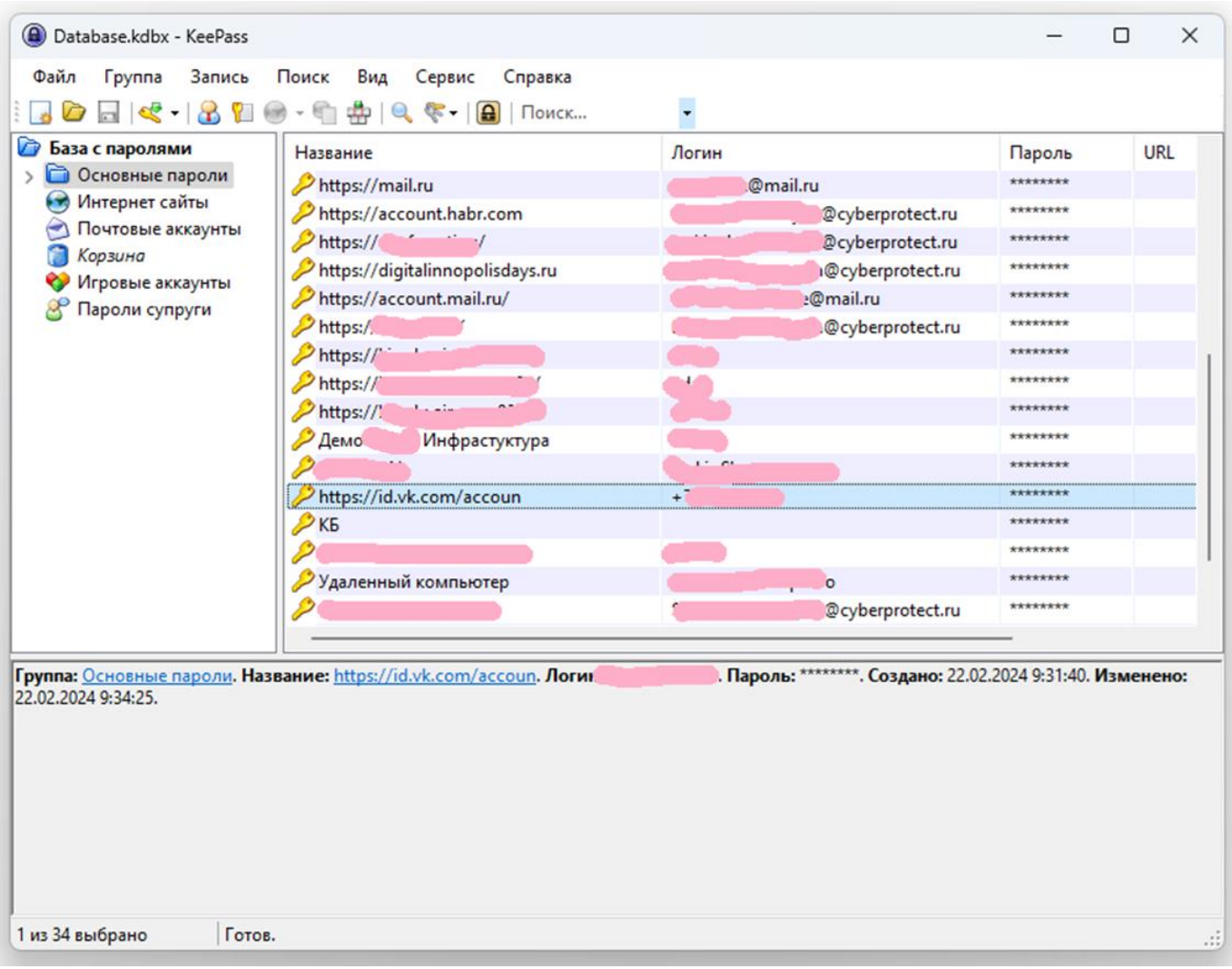
Двухфакторная аутентификация (2FA) – способ идентификации пользователя в каком-либо сервисе, при котором нужно предъявить два разных типа аутентификационных данных

Второй фактор аутентификации:

- ☑ Одноразовый код (СМС, ОТР, заранее сгенерированные коды)
- ☑ Биометрия (отпечатки, лицо, сетчатка глаз, голос)
- ☑ Аппаратный ключ
- ☑ Местоположение

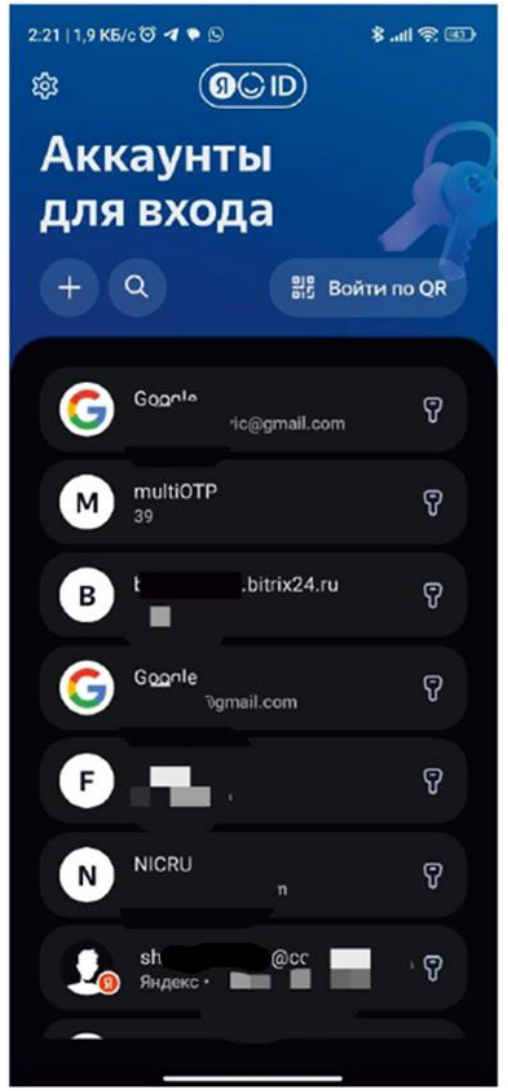
ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

KeePass



+

Яндекс Ключ



КИБЕРПРОТЕКТ

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

ОДНИ «ДЫРЫ» ВЗАМЕН ДРУГИХ...

СОБЛЮДАЙТЕ ВАЖНЫЕ ПРИНЦИПЫ:

- ☑ Регулярно устанавливайте обновления ПО
- ☑ Обновляйте прошивки роутеров
- ☑ Меняйте реквизиты доступа по умолчанию от разных устройств
- ☑ Используйте непривилегированные аккаунты

ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ!

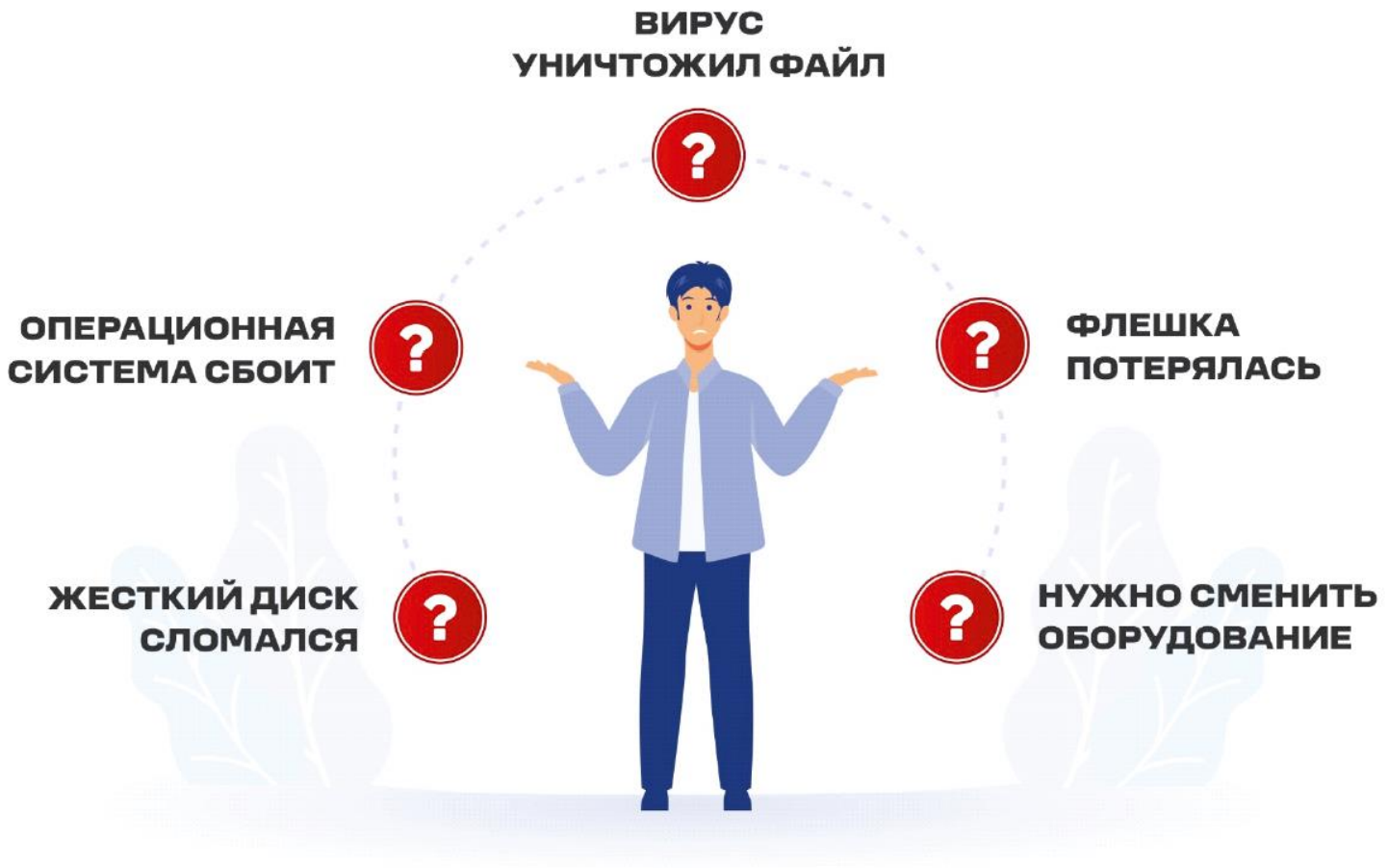
Антивирусы и встроенные средства защиты

Используйте антивирусы и встроенные средства защиты, регулярно обновляйте ПО

Цели вирусов:

- Кража учетных и персональных данных
- Кража финансовых данных и денег
- Шифрование и шантаж для получения выкупа
- Превращение устройства в зомби, бота. Используется для рассылки спама, массовых атак на сайты, майнинга криптовалют и т.п.

ДАННЫЕ ТЕРЯЮТСЯ



**ЧТОБЫ ОБЕЗОПАСИТЬ СЕБЯ ОТ ПОТЕРИ ВАЖНОЙ ИНФОРМАЦИИ,
НУЖНО ИМЕТЬ РЕЗЕРВНУЮ КОПИЮ ДАННЫХ**

ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ!

Создавайте резервные копии ваших данных!

Привилегией цифрового мира является возможность создания резервных копий и восстановления важной информации в случае ее потери

Руководствуйтесь правилом 3-2-1:

- ☑ Иметь **3 копии** данных
- ☑ Хранить копии на **2 разных носителях**
- ☑ Хранить **1 резервную копию** в облаке

КИБЕРПРОТЕКТ

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ!

Контроль каналов утечки, данных, хранилищ, сотрудников

Контроль в реальном времени

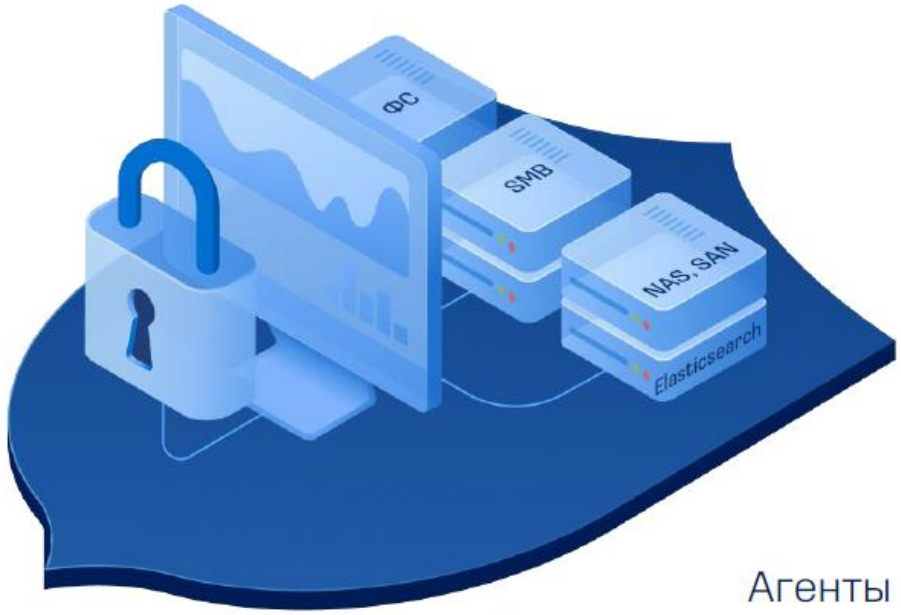
При использовании и передаче данных

Агенты системы DLP

На физических рабочих станциях и серверах, виртуальных и терминальных средах

Превентивный контроль

При хранении данных



Агенты обнаружения данных

В хранилищах

На сервере – удалённое сканирование хранилищ

КИБЕРПРОТЕКТ

Эксклюзивы РБК, 10 янв, 00:00 | 63 789 | Поделиться | ЭКСКЛЮЗИВ

Вымогатели начали использовать ИИ для подделки голосовых в Telegram Чем новая схема опасна для пользователей

Мошенники начали вымогать деньги созданными с помощью ИИ аудиосообщениями

Сюжет
Эксклюзивы РБК

Мошенники генерируют с помощью ИИ голосовые обращения на основе аудиосообщений владельцев аккаунта — это позволяет убедительнее просить деньги у его знакомых. Эксперты называют такую схему новой для России, но сложной в исполнении

НОВОСТИ ВОРОНЕЖА

9 июля 2024 года
вторник

Пробки
3 балла

USD ЦБ 88,17 +0,03
EUR ЦБ 95,66 +0,09

Главная | Общество | Политика | В России | Происшествия | Тел

15:46 24 января 2024

Воронежская пенсионерка отдала мошенникам 100 тысяч, помогая своей соседке

Доверчивая женщина думала, что помогает знакомой

Женщина лишилась крупной суммы.
Автор: Алена Орехова. Фото: из архива.

Доверчивая пенсионерка из Воронежа хотела помочь попавшей в беду соседке. Вот только в реальности её обманули мошенники, которым она отдала крупную сумму. Об этом в среду, 24 января 2024 года сообщили в МВД.

Оказалось, что 89-летней женщине поступило голосовое сообщение якобы от соседки. Та сказала, что попала в ДТП и сбила человека. Она сообщила, что сама сейчас в больнице и ей срочно нужны деньги для передачи потерпевшей.

После этого пенсионерке звонили разные люди, представлявшиеся полицейскими и медиками. Они просили деньги на вещи для больницы и другие нужды

Мошенники подделали голос родственника и «одолжили» у жертвы 100 тыс. рублей

23 января 2024, 12:59
3114

МОШЕННИЧЕСТВО МЕССЕНДЖЕРЫ TELEGRAM ДЕНЬГИ

Красная шапочка из Подмосковья: мошенники прикинулись бабушкой и обманули ребенка на большую сумму денег

- Случаи мошенничества, когда жертвами становятся взрослые люди, в последнее время не редкость. Однако история мошенничества произошла с 11-летней школьницей из подмосковного Королева.

КИБЕРПРОТЕКТ

ИА «НТА Приволжье»

ПОЛИТИКА И ВЛАСТЬ

Мошенники создали фейковый аккаунт главы Дзержинска

Нижний Новгород. 8 февраля. НТА-Приволжье — Мошенники создали фейковый аккаунт главы Дзержинска.

О действиях злоумышленников написал в своем телеграм-канале глава Дзержинска Иван Носков.

"Все, кто общается со мной через телеграм – внимательно проверяйте, от кого пришло сообщение. Я не менял свой номер телефона!" - заявил Иван Носков.

"Не отвечайте, не задавайте уточняющих вопросов сомнительным контактам, вступайте с ними в переписку и незамедлительно блокируйте фейковый аккаунт!"- сказал Иван Носков.

Ранее сообщалось, что фейковый аккаунт Глеба Никитина появился в сети.

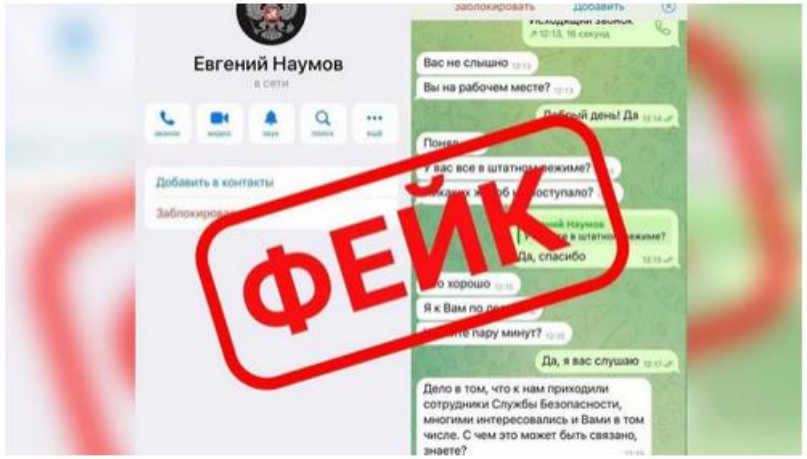
"Кто общается со мной лично, перепроверяйте, с какого аккаунта пришло сообщение. Не вступайте в переписку, и поддельный аккаунт блокируйте", - заявил губернатор Нижегородской области Глеб Никитин.

НОВОСТИ Политика Экономика Общество Ещё

4 апреля Комсомольская правда Общество

Мошенники рассылали сообщения от имени главы Краснодара

Глава Краснодара предупредил о фейковой странице, созданной мошенниками под его именем.



Источник: Евгений Наумов | глава Краснодара — Telegram

Мошенники рассылали сообщения от имени главы Краснодара. Об этом Евгений Наумов сообщил в официальном telegram-канале.

«Мошенники с фейковой страницы снова пишут от моего имени. Перед тем как вступать в переписку, проверяйте номер. А лучше позвоните по нему», — отметил глава города.

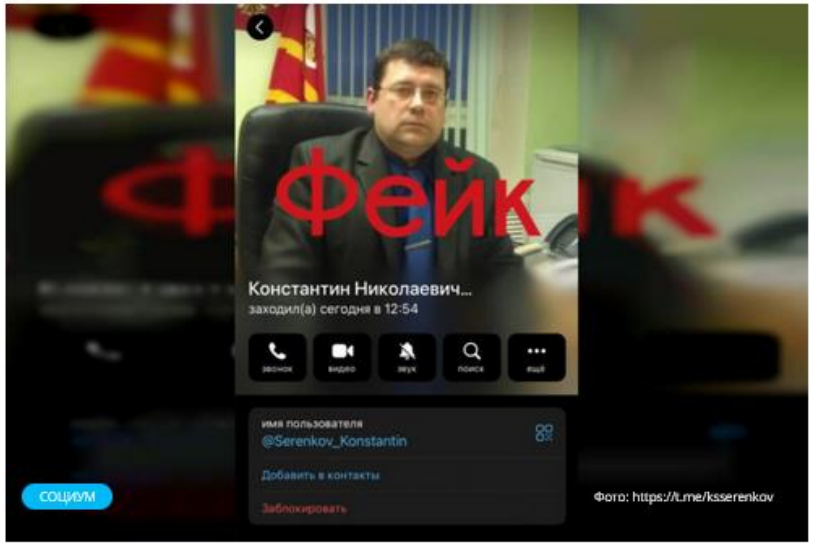
Жителей призывают быть бдительными и не забывать про информационную гигиену.

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

СМОЛЕНСКАЯ НАРОДНАЯ ГАЗЕТА

Мошенники общались с людьми от имени главы одного из смоленских муниципалитетов



АВТОР
Катя Миглина

ОПУБЛИКОВАНО
31.01.2024

Это пятый подобный случай с начала года

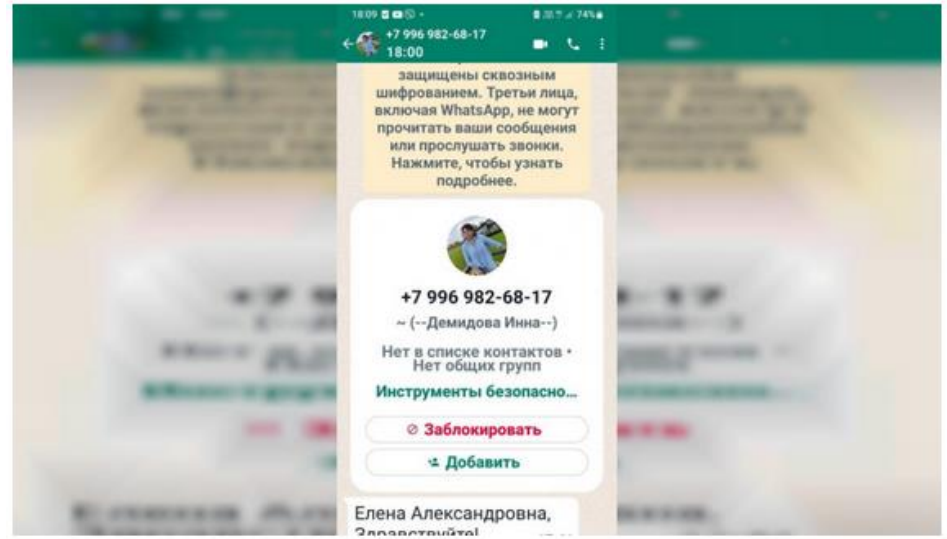
В Telegram появился фейковый аккаунт главы Дорогобужского района Константина Серенкова. Чиновник сообщил об этом в своих официальных соцсетях в среду, 31 января.

По словам Константина Николаевича, мошенники уже начали общаться с некоторыми его друзьями с фейкового аккаунта. Глава района попросил не отвечать фальшивому "Серенкову" и блокировать учетную запись.

Это не первый случай создания фейков смоленских чиновников. За минувший месяц зарегистрировано минимум пять фальшивых аккаунтов.

Первым был фейк главы Вяземского района Инны Демидовой. Тогда фальшивку создали в WhatsApp.

Мошенники притворились главой одного из смоленских муниципалитетов



ПРОИСШЕСТВИЯ

АВТОР
Катя Миглина

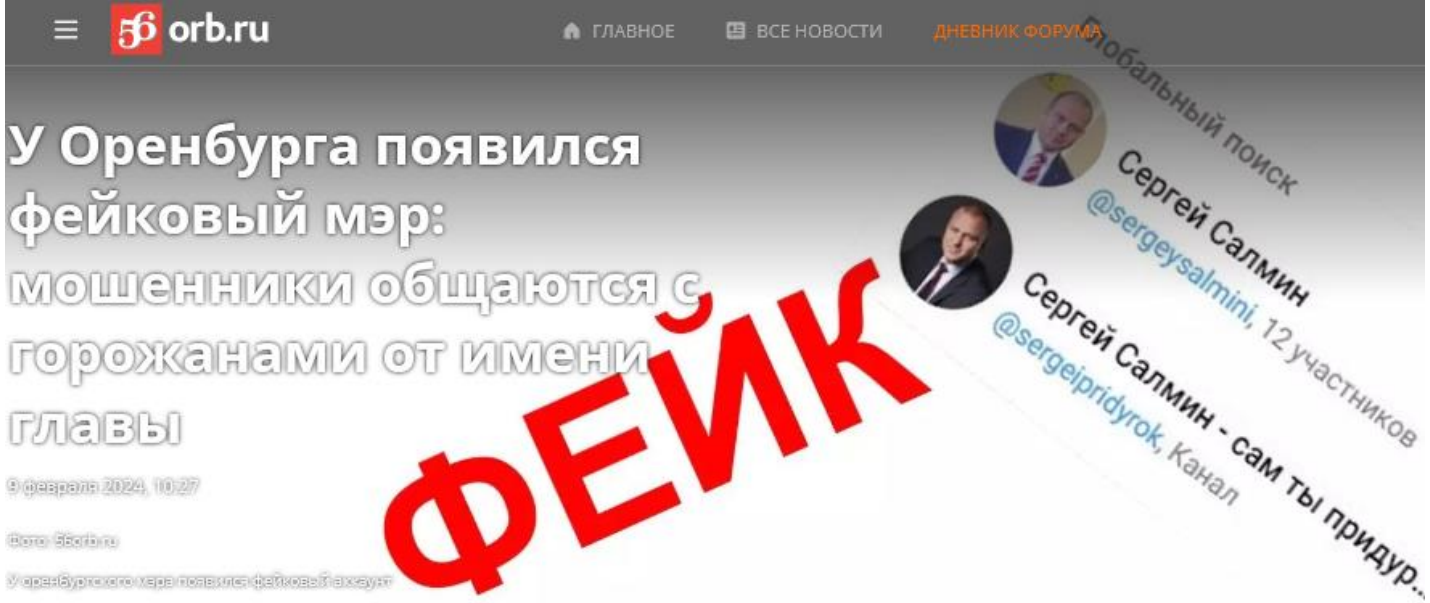
ОПУБЛИКОВАНО
17.01.2024

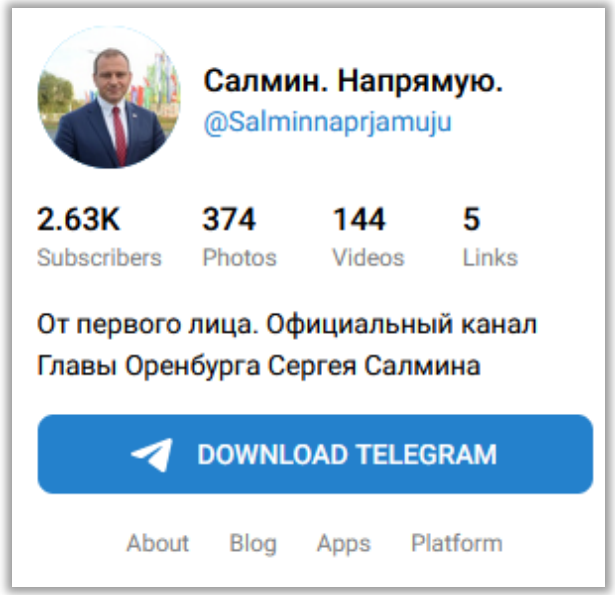
Фальшивый аккаунт создали в мессенджере

В WhatsApp появился фейковый аккаунт главы Вяземского района, Инны Демидовой. Об этом глава муниципалитета сообщила в своём Telegram-канале.

Аккаунт, названный Демидовой Инной, проявился, написав третьему лицу. Номер фальшивой Инны: +79969826817. Отметим, что согласно ресурсу https://my-operator.info/ номер зарегистрирован в Нижегородской области. С главой муниципалитета аккаунт никак не связан.

> *"Если вам будут приходить сообщения с этого номера, отвечать на них не нужно. Любую информацию лучше подвергнуть сомнению и перепроверить. Пожалуйста, будьте внимательны!"* — пишет настоящая Инна Васильевна.





У оренбургского мэра появился фейковый аккаунт в соцсетях

Мэр Оренбурга в своем тг-канале рассказал о том, что мошенники создали аккаунт от его имени. Кому не отвечать на сообщения — расскажем подробнее.

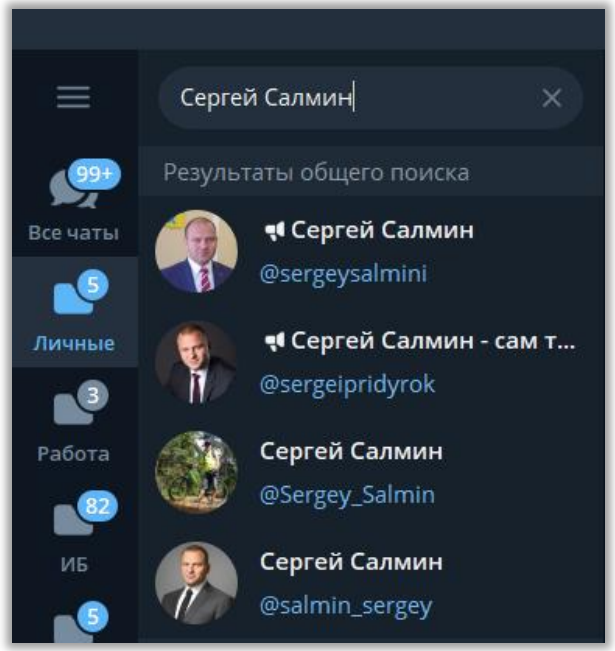
Сюжет

Город

Сегодня мэр Оренбурга Сергей Салмин в своем тг-канале обратился к оренбуржцам вот с таким заявлением:

> **— Уважаемые горожане, коллеги! Обращаю внимание: мошенники создали мой фейковый аккаунт в Telegram с моим именем и фотографией. Прошу вас не реагировать, в переписку не вступать, по ссылкам не переходить и незамедлительно блокировать фейковый аккаунт! Всех, кто общается со мной лично, прошу проверять аккаунт, с которого поступает сообщение.**

В свою очередь, хочется отметить, что это не первый поддельный аккаунт мэра Оренбурга. В Telegram как минимум две странички с фотографией и именем Сергея Салмина.



56orb.ru
11,3К подписчиков
Подписаться

В Оренбургской области мошенники заговорили голосом главы города

21 февраля

В очередной раз злоумышленники добрались до оренбургских чиновников. В Telegram-канале мошенники создали аккаунт от имени главы Бузулука Владимира Пескова.

В очередной раз злоумышленники добрались до оренбургских чиновников. В Telegram-канале мошенники создали аккаунт от имени главы Бузулука Владимира Пескова.

Глава Бузулука Владимир Песков пояснил, что злоумышленники использовали его имя и фотографию. После стали массово рассылать сообщения с просьбой позвонить по неизвестным номерам. Мошенникам удалось даже записать аудиосообщение якобы от имени главы города.

> — ***Мошенники записали голосовые сообщения, и голос очень сильно похож, но все же слышно, что это компьютерная обработка,*** — *заявил Владимир Песков в своем официальном аккаунте.*

Глава Бузулука попросил жителей Оренбуржья не отвечать на подобные звонки и сообщения. Песков подчеркнул, что у него только один официальный профиль.

НОВОСТИ Политика Экономика Общество События Все сервисы
4 апреля · Комсомольская правда · Общество

Мошенники рассылали сообщения от имени главы Краснодара

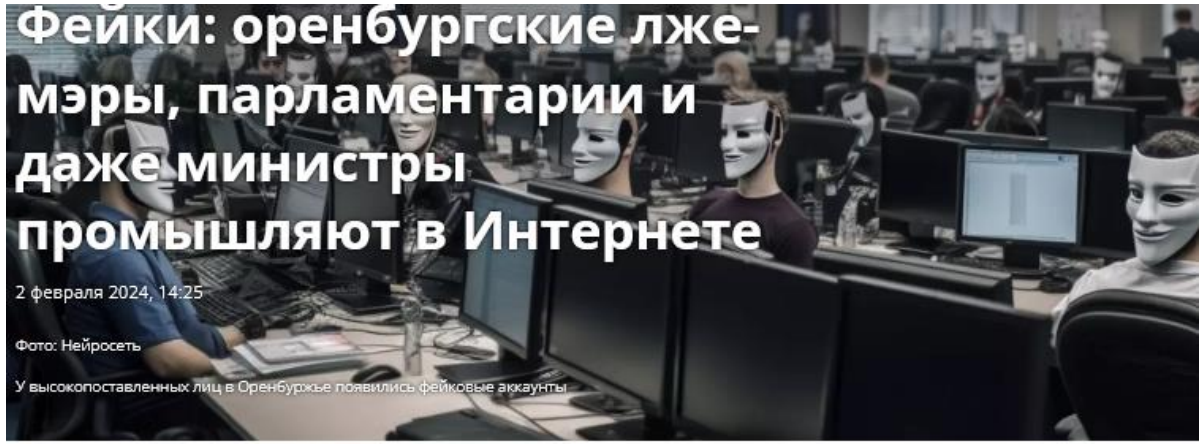
Глава Краснодара предупредил о фейковой странице, созданной мошенниками под его именем.

Источник: Евгений Наумов | глава Краснодара — Telegram

Мошенники рассылали сообщения от имени главы Краснодара. Об этом Евгений Наумов сообщил в официальном telegram-канале.

«Мошенники с фейковой страницы снова пишут от моего имени. Перед тем как вступать в переписку, проверяйте номер. А лучше позвоните по нему», — отметил глава города.

Жителей призывают быть бдительными и не забывать про информационную гигиену.



Фейки: оренбургские лже-мэры, парламентарии и даже министры промышляют в Интернете

2 февраля 2024, 14:25

Фото: Нейросеть

У высокопоставленных лиц в Оренбуржье появились фейковые аккаунты

Оренбуржцев просят не отвечать на сообщения от мэров, министров и парламентариев

Оренбургские випы все чаще становятся объектами мошенников в Интернете. Фейковые страницы завели уже как минимум от имени мэра, министра и двух парламентариев. Подробности далее.

Сюжет

Город

В социальных сетях и мессенджерах в последнее время стали появляться ненастоящие аккаунты разных руководителей и чиновников из Оренбуржья. ФСБ констатирует увеличение количества попыток мошенников завладеть персональными данными сотрудников медицинских, образовательных и других государственных учреждений. И, конечно, мошенникам важно проникнуть в систему организации, которой руководит заинтересовавший злоумышленников.

Цели могут быть разными. От хищения денег до промышленного и государственного шпионажа. А в целом, атакам мошенников сейчас подвергаются абсолютно все категории граждан. Молодежь, пенсионеры, люди среднего возраста. В независимости от социального статуса и положения в обществе.

> **— Уважаемые горожане, коллеги! Мошенники создали в социальной сети Telegram фейковый аккаунт с моей фамилией и фотографией. Рассылают глупые просьбы от моего имени. Прошу вас не реагировать, в переписку не вступать, по ссылкам не переходить и отправлять нехороших людей в спам. Обратился к администраторам социальной сети с просьбой заблокировать мошенника. Козупица Василий Николаевич, только здесь. Настоящий. Ваш.**

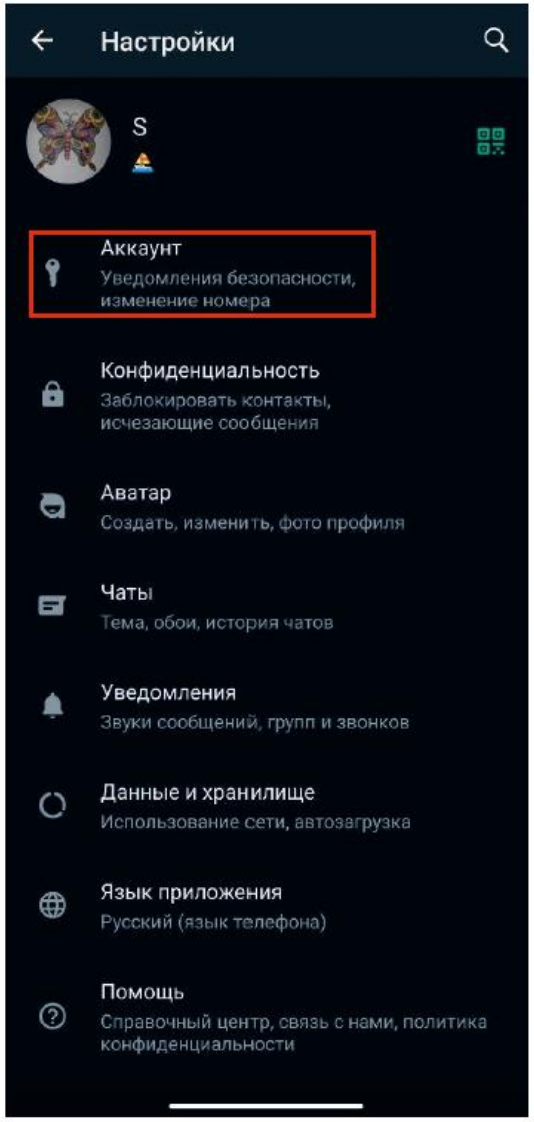
Мэр Орска даже переименовал свою страничку соответственно: Настоящий Козупица. Наверное, чтобы горожане уж точно не перепутали с тем другим, ненастоящим.

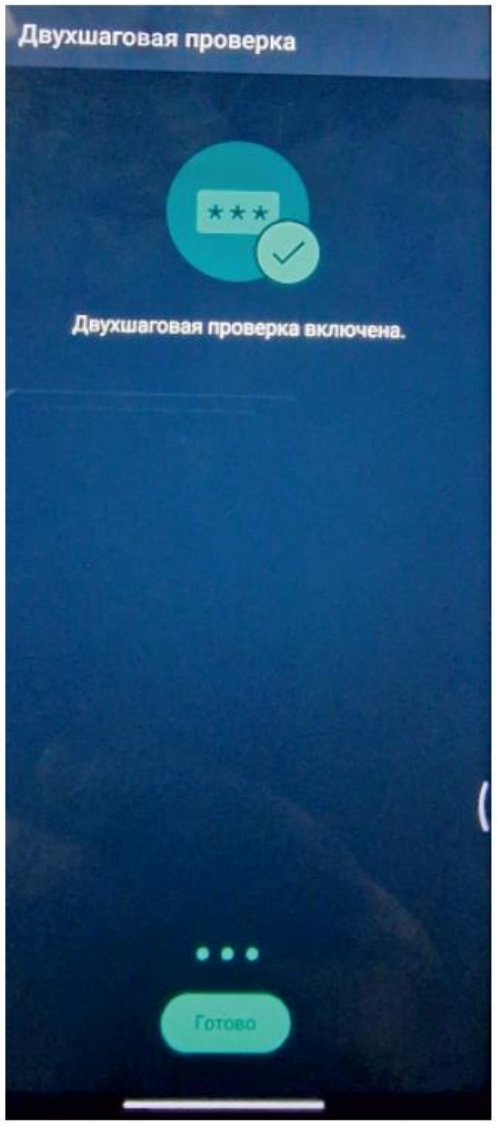
У вице-губернатора Игоря Сухарева тоже появился фейковый аккаунт. И в тг-канале Сухарев Press он обратился к своим подписчикам с просьбой не реагировать на странные сообщения от его имени.

ЗАЩИТА АККАУНТА WHATSAPP

1. Перейдите в «Настройки»
2. Нажмите «Аккаунт»
3. Нажмите «Двухшаговая проверка»
4. Нажмите кнопку «Включить»
5. Придумайте и укажите 6-ти значный ПИН. Введите его 2 раза. Нажмите «Далее»
6. Система предложит указать электронный почтовый адрес, на который будет направлен код восстановления доступа к аккаунту Whatsapp, если вы забудете ПИН. Введите его 2 раза. Нажмите «Далее»
7. Нажмите «Готово».

НАДЕЖНО ХРАНИТЕ ПИН!

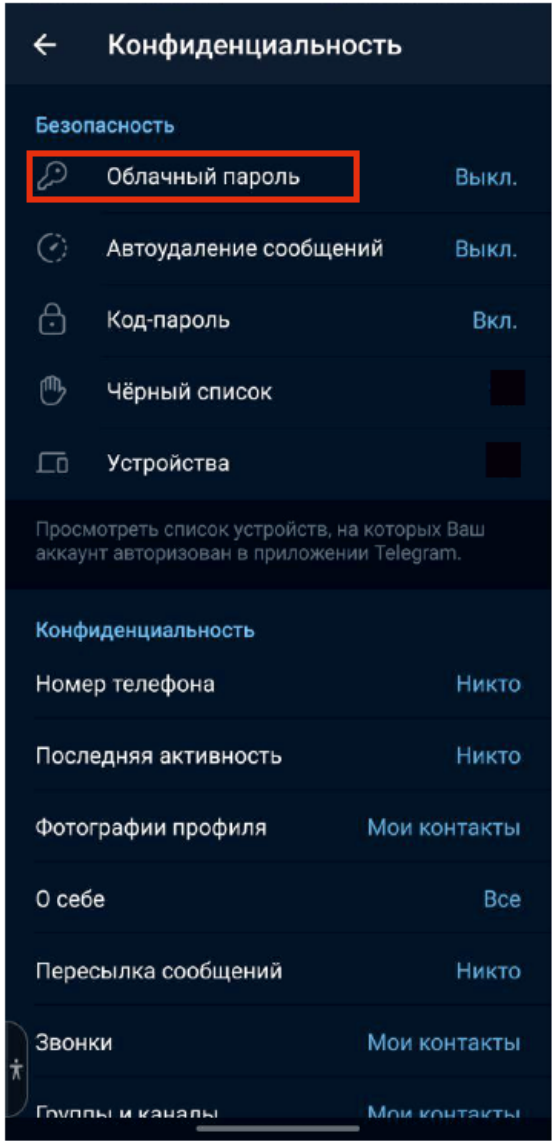




ЗАЩИТА АККАУНТА ТЕЛЕГРАММ

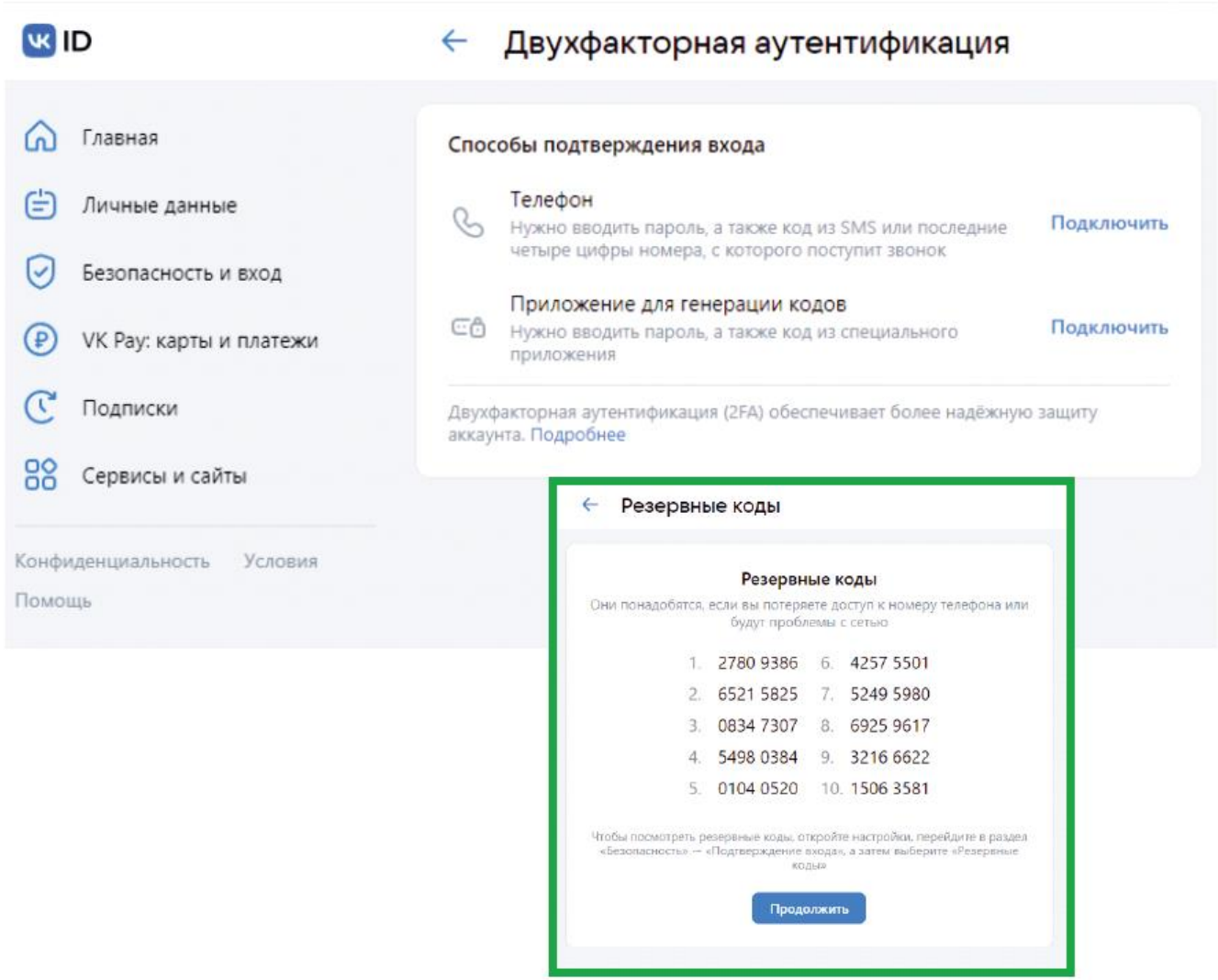
1. Перейдите в «Настройки»
2. Нажмите «Конфиденциальность»
3. В разделе «Безопасность» нажмите «Облачный пароль»
4. Далее задайте пароль следуя инструкции на экране
5. Введите подсказку для напоминания пароль
6. Рекомендуется ввести неактуальные подсказки
7. Система предложит указать электронный почтовый адрес, на который будет направлен код восстановления доступа к аккаунту Телеграмм, если вы забудете «Облачный пароль»
8. Введите код, направленный на почтовый адрес, в форму Телеграмма для завершения установки «Облачного пароля»

НАДЕЖНО ХРАНИТЕ ОБЛАЧНЫЙ ПАРОЛЬ!



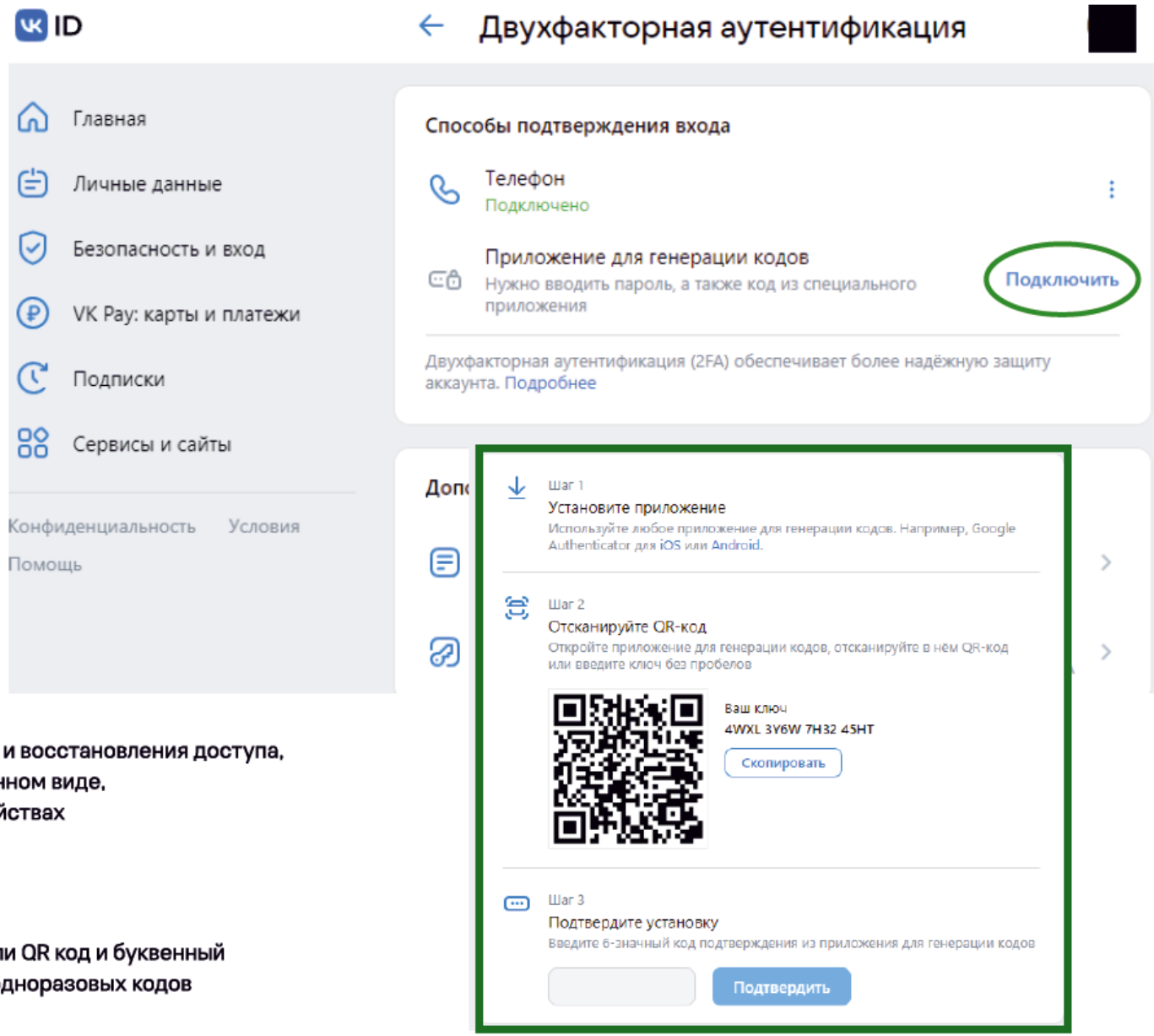
ЗАЩИТА АККАУНТА ВКОНТАКТЕ

1. Войдите в свой аккаунт **VK.COM** через браузер
2. Перейдите в «Настройки»
3. Далее нажмите на «Безопасность»
4. В разделе «Безопасность и вход» проверьте правильность указанного телефона и электронной почты
5. В пункте «Способы входа» нажмите «Двухфакторная аутентификация»
6. Нажмите «Подключить» напротив пункта «Телефон»
7. Введите запрошенные данные для включения двухфакторной аутентификации



ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ!

1. Зайдите по адресу **https://vk.com**
2. Перейдите в раздел «Настройки»
3. Перейдите в раздел «Безопасность»
4. В блоке «Способы входа» нажмите «Двухфакторная аутентификация»
5. В блоке «Приложение для генерации кодов» нажмите подключить
6. Введите пароль от аккаунта
7. Установите приложение для генерации одноразового кода и отсканируйте QR код
8. Введите одноразовый код из приложение в поле «Подтвердить установку» и нажмите «Подтвердить»



1. Внимательно читайте и выполняйте инструкции от сервиса при подключении 2FA через приложение
2. Указывайте ваши реальные: ФИО, телефон и почтовый адрес
3. Храните одноразовые коды в надежном месте. Они нужны для входа и восстановления доступа, если приложение-генератор кода недоступно. Если храните в электронном виде, сделайте несколько резервных копий файла с кодами на разных устройствах

Важно:

- настройку 2FA в аккаунтах осуществляйте на своих устройствах,
- пароли вводите так, чтобы НИКТО не видел
- сделайте так, чтобы НИКТО (в т.ч. технические специалисты) не видели QR код и буквенный код, предназначенный для подключения 2FA приложения-генератора одноразовых кодов

ЗАЩИТИТЬСЯ НЕЛЬЗЯ ИГНОРИРОВАТЬ
КОМПРОМЕТАЦИЮ ДАННЫХ

- ☑ Подтверждение официального статуса канала в социальных сетях (Вконтакте, Телеграм)
- ☑ На сайте НКО собрать все официальные страницы для общественности с быстрым доступом и доступной информацией
- ☑ Иметь стандартный номер телефона и везде его публиковать (сайты, соц.сети, справочники, карты, пр.)
- ☑ Учиться и учить защите от актуальных цифровых угроз, навыкам цифровой гигиены коллег и общественность

Учение — только свет, по народной пословице, — оно также и свобода.

Ничто так не освобождает человека, как знание».

Иван Сергеевич Тургенев

Учите и учитесь!

ЗЛОУМЫШЛЕННИКИ АТАКУЮТ

САМАЯ УЯЗВИМАЯ ЧАСТЬ СИСТЕМЫ

ИНЖЕНЕРИЯ, ДА НЕ ПРОСТАЯ, А СОЦИАЛЬНАЯ

Социальная инженерия — это совокупность психологических методик и мошеннических приемов для создания условий, при которых возможно манипулирование человеческим сознанием и поведением.

Основные векторы:

- Сообщением (электронная почта, сообщения через СМС (смишинг) и мессендежры)
- Голосом, он же ВИШИНГ (телефонные звонки, записи высказываний, и пр.)

ИНЖЕНЕРИЯ, ДА НЕ ПРОСТАЯ, А СОЦИАЛЬНАЯ

Три кита социальной инженерии

- Достучаться до человека: почта, мессенджеры, социальные сети, телефон
- Вызвать яркую эмоцию. Мошенники знают все наши «грехи»:
  - Страх потери и тревога за близких
  - Алчность и любовь к халяве
  - Сострадание и чувство вины
  - Внимание со стороны красивого или обеспеченного человека
- Использовать текущий контекст

ИНЖЕНЕРИЯ, ДА НЕ ПРОСТАЯ, А СОЦИАЛЬНАЯ

Основные правила противодействия сетевым мошенникам:

- Помните: Вы никому ничего не обязаны! Относитесь ко всему происходящему вокруг вас критично!
- Ничего не отвечайте, не кликайте, не устанавливайте, не делитесь в ответ на странные запросы или запросы от неизвестных лиц
- Пользуйтесь на своих устройствах антивирусными решениями и блокираторами мошеннических звонков
- Постоянно интересуйтесь новыми мошенническими схемами, приемами и способами защиты от них. Делитесь информацией с родными и близкими!

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ, С НАЛЁТОМ DEEPFAKE

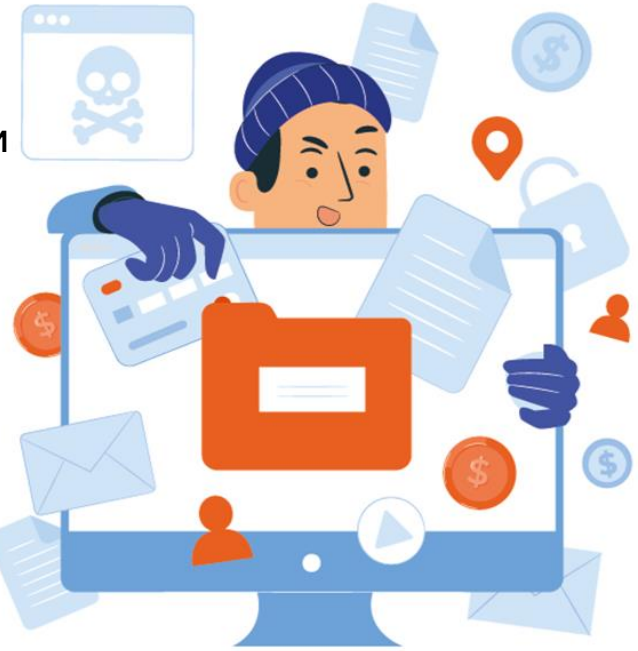
Как защититься от атак voice deepfakes (подделка голоса) частным лицам?

- Критически относитесь к любой информации в мессенджерах, соцсетях и почте, даже от знакомых
- Удалять голосовые сообщения
- Не публиковать видео со своим голосом
- Придумать секретный код или пароль, для дополнительной идентификации с близкими друг друга
- Прослушивая запись обращаться внимания на звучание речи, равномерность, схожесть с речью известного вам человека – это может указать на подделку
- Включить автоудаление переписки

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ, С НАЛЁТОМ DEEPFAKE

Как защититься от атак voice deepfakes (подделка голоса) представителям НКО?

- Подтвердить статус официального канала (через средства Telegram, VK,
- Для работы применять утвержденную систему внутренней коммуникации и обмена данными
- Критически относитесь к любой информации в мессенджерах, соцсетях и почте, даже от знакомых
- ~~Удалять голосовые сообщения~~
- ~~Не публиковать видео со своим голосом~~
- Придумать секретный код или пароль, для дополнительной идентификации вас, коллег и руководителя
- Прослушивая запись обращаться внимания на звучание речи, равномерность, схожесть с речью известного вам человека – это может указать на подделку
- ~~Включить автоудаление переписки~~



НАУЧИТЕСЬ РАСПОЗНАВАТЬ «СВОЙ-ЧУЖОЙ»!

- Применять все встроенные механизмы защиты аккаунтов (многофакторную аутентификацию, дополнительный номер телефона, др.) для всей цепочки аккаунтов:
  Соцсеть → *электронная почта* → *способы восстановления доступа* → *резервная почта*
- Анализировать характер просьб/поручений на предмет срочности, неожиданности, нетипичности и иных аномалий
- Связаться с отправителем сообщения иным каналом связи, желательно, с другого устройства, подтвердить запрос
- Заблаговременно предлагать общественности подписаться на официальные каналы НКО и их представителей
- На официальном сайте явно указать адреса со всеми официальными (настоящими) аккаунтами представителей и самих НКО. Позиционировать данную площадку как место для подтверждения легальности аккаунтов
- Разместить сайт на отечественной хостинг площадке, разрешить доступ из России (по принципу минимального)

НАУЧИТЕСЬ РАСПОЗНАВАТЬ «СВОЙ-ЧУЖОЙ»!

Фишинг — вид интернет-мошенничества,
цель которого получить данные пользователей

Механизмы:

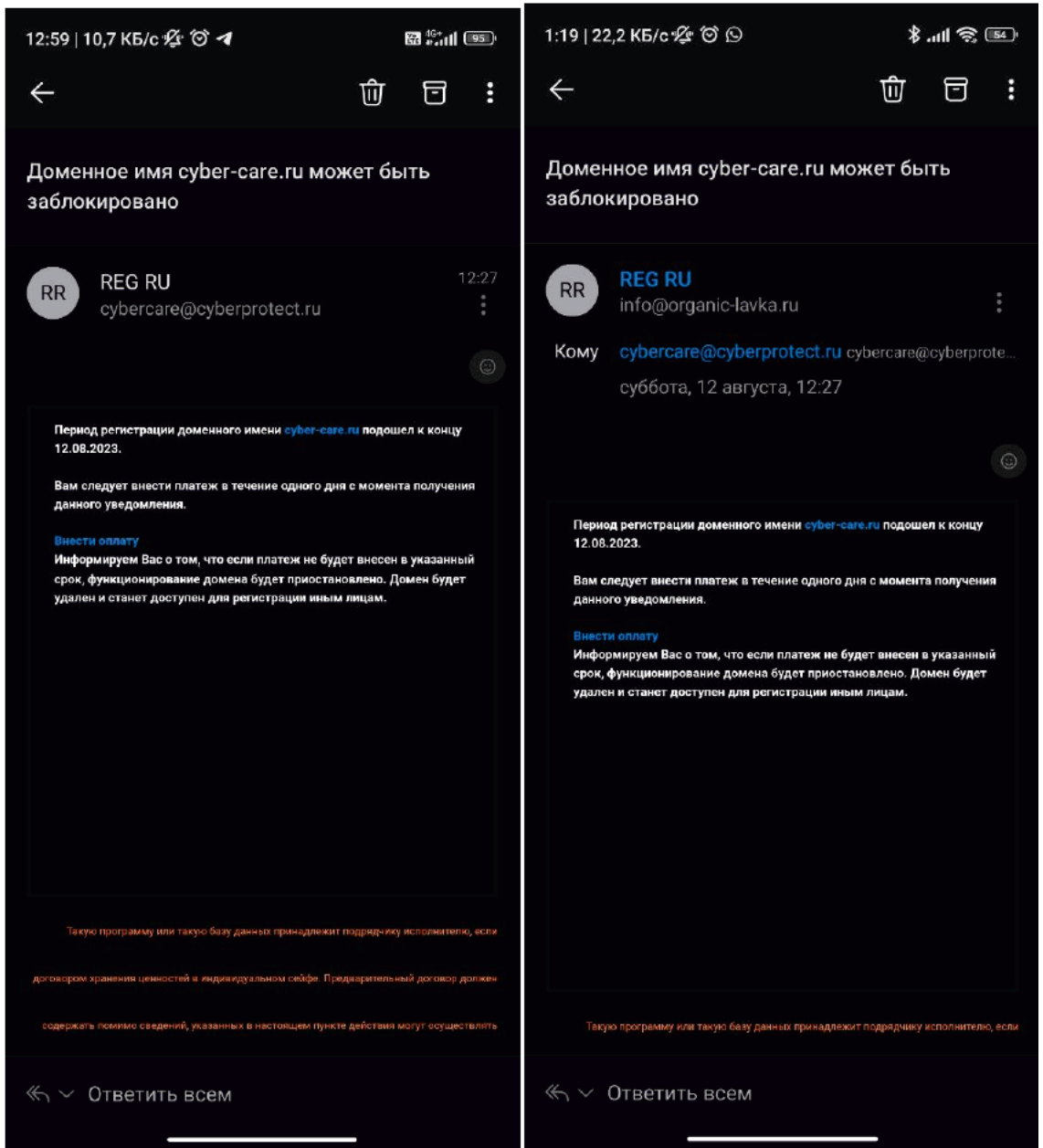
- Поддельная ссылка
- Вредоносное содержимое
- Ложные легенды

НАУЧИТЕСЬ РАСПОЗНАВАТЬ «СВОЙ-ЧУЖОЙ»!

Фишинг — вид интернет-мошенничества, цель которого получить данные пользователей

Механизмы:

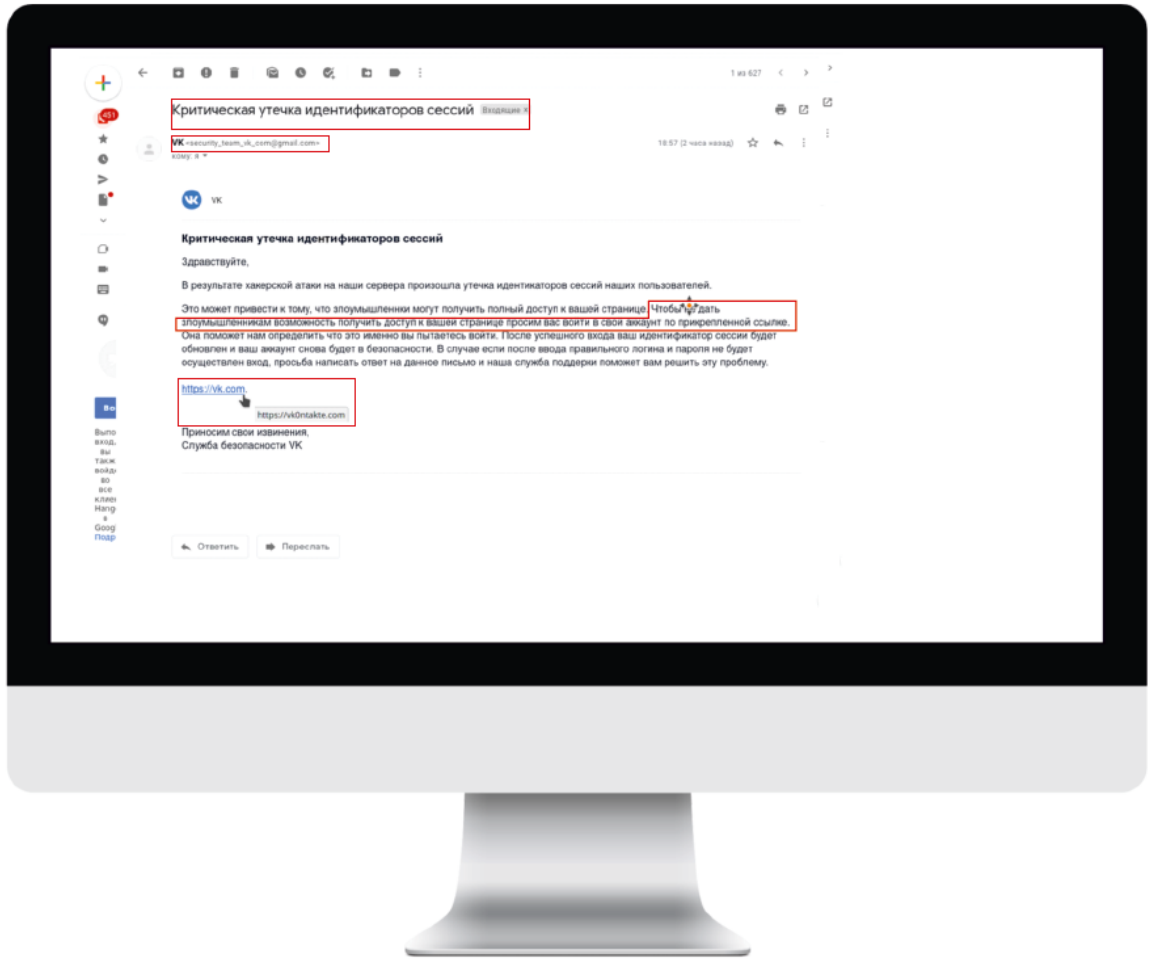
- Поддельная ссылка
- Вредоносное содержимое
- Ложные легенды



НАУЧИТЕСЬ РАСПОЗНАВАТЬ «СВОЙ-ЧУЖОЙ»!

Как определить фишинговое письмо

- Неизвестный отправитель
- Кричащая тема письма
- Обезличенное обращение или автоподстановка имени
- В письме проблема или срочный вопрос – от вас требуется немедленное действие
- Запрашивают личные данные или банковские реквизиты
- Предложение слишком хорошо, чтобы быть правдой
- В письме есть вложения, файлы (маленький размер файла, архив zip и rar)
- Содержит подозрительную ссылку
- Обезличенная подпись



СТАВЬТЕ ВСЁ ПОД СОМНЕНИЕ

Социальная инженерия. Самый высокий уровень результативности демонстрируют атаки методами социальной инженерии совместно с фишинговыми ресурсами и вредоносными приложениями

Вредоносное ПО. Применение вредоносного ПО является инструментом нарушения конфиденциальности, целостности и доступности данных, внедрение и закрепление в сети организации, ИСПДН, др.
От вирусов-шифровальщиков защищает, преимущественно, правильно организованная система резервного копирования данных

Дипфейки. Технологии ИИ могут использовать и злоумышленники, чтобы подделать лицо и голос. При поступлении подозрительных просьб через звонки и аудиовизуальные сообщения в мессенджерах лучше перезвоните контрагенту и задайте уточняющие вопросы.

Социальная ответственность Киберпротекта

НАЦИОНАЛЬНЫЕ ПРОЕКТЫ РОССИИ

ПАРТНЕР

КИБЕРПРОТЕКТ

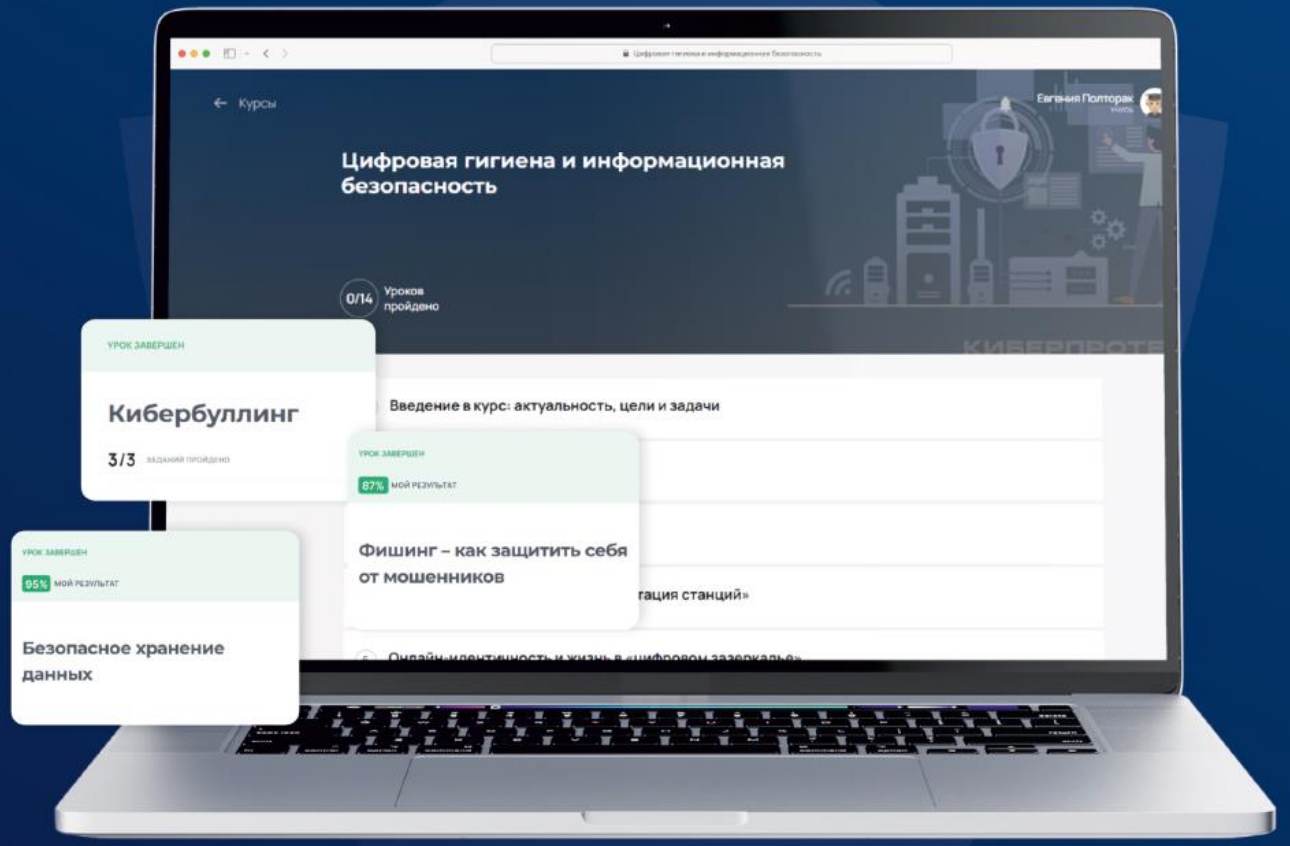
Призёр премии

#МЫВМЕСТЕ

КИБЕР Забота

Всероссийский проект по обучению детей и взрослых принципам безопасного поведения в сети Интернет

https://cyber-care.ru



КИБЕРПРОТЕКТ

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

Академическая программа

Работа с вузами и колледжами

- Бесплатный доступ к ПО для применения в учебном процессе
- Предоставляем учебно-методические материалы
- Проводим бесплатное обучение и сертификацию педагогов
- Бесплатный доступ для студентов к вендорской сертификации

academy@cyberprotect.ru

Вместе готовим кадры для экономики данных

КИБЕРПРОТЕКТ

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

КИБЕРПРОТЕКТ

Спасибо за внимание

Канал компании Киберпротект

TG: @cyberprotect.ru

Cyberprotect.ru